数学机械化丛书

实域论

曾广兴 著

科学出版社
www.sciencep.com

(O-1836.0101)

数学机械化丛书(部分书目)

- 数学机械化　吴文俊
- 几何定理机器证明的几何不变量方法　张景中、高小山、周咸青
- 消去法及其应用　王东明
- 组合恒等式的机器证明　陈永川
- 几何自动作图与智能CAD　高小山
- 代数曲面造型　陈发来 等
- 非线性数学物理方程的行波解　李志斌 等
- 实域论　曾广兴



ISBN 7-03-012089-2
定价: 50.00 元

数学机械化丛书

实　　域　　论

曾广兴　著

科学出版社
北　京

内 容 简 介

本书旨在比较系统地介绍实域理论中的内容、方法和结论. 对于进一步学习实代数几何的人来说，本书应是一本必读物.

全书共分 9 章. 前两章围绕著名的 Artin-Schreier 理论，介绍与实域、序域和实闭域相关的概念和结论. 第三章讨论了域的实赋值和实位以及它们与序之间的相容性. 第四章介绍 E. Artin 对 Hilbert 第十七问题的解答，同时研究了 Hilbert 第十七问题的逆问题. 第五章讨论了实域上的二次型及其密切相关的半序，由此建立了一些重要的结果，其中包括 Hilbert 第十七问题在定量方面的结论. 在第六章中，几类特殊的实域和序域被研究，这些域包括 SAP 域、欧氏域、遗传欧氏域、Pythagoras 域和遗传 Pythagoras 域等. 第七章介绍了适合实闭域的 Tarski-Seidenberg 原理与转移原理，并应用于实零点定理的建立. 第八章涉及域的高层序理论， Artin-Schreier 理论在此获得推广. 在第九章中，一些与实域理论有关的构造性结论被介绍，其中包括柱形代数分解和半正定多项式的判定等.

本书可作为代数专业的研究生教材，也可供专业研究人员参考.

图书在版编目（CIP）数据

实域论 / 曾广兴著. —北京：科学出版社， 2003
(数学机械化丛书 / 吴文俊主编)
ISBN 7-03-012089-2

Ⅰ. 实… Ⅱ. 曾… Ⅲ. 实数域 Ⅳ. O156.2

中国版本图书馆 CIP 数据核字 (2003) 第 074135 号

责任编辑：吕 虹 / 责任校对：陈丽珠
责任印制：钱玉芬 / 封面设计：黄华斌 陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com
中国科学院印刷厂 印刷
科学出版社编务公司制作
科学出版社发行 各地新华书店经销
*
2003年12月第 一 版 开本：B5(720×1000)
2003年12月第一次印刷 印张：23 1/4
印数：1－2 500 字数：420 000

定价：50.00 元

(如有印装质量问题，我社负责调换〈科印〉)

《数学机械化丛书》获国家基础研究发展规划项目“数学机械化与自动推理平台”与“数学机械化应用推广专项经费”资助

《数学机械化丛书》编委会

《数学机械化丛书》前言[①]

16,17 世纪以来，人类历史上经历了一场史无前例的技术革命，出现了各种类型的机器，取代各种形式的体力劳动，使人类进入一个新时代. 几百年后的今天，电子计算机已开始有条件地代替一部分特定的脑力劳动，因而人类已面临另一场更宏伟的技术革命，处在又一个新时代的前夕. 数学是一种典型的脑力劳动，它在这一场新的技术革命中，无疑将扮演一个重要的角色. 为了了解数学在当前这场革命中所扮演的角色，就应对机器的作用，以及作为数学的脑力劳动的方式，进行一定的分析.

1. 什么是数学的机械化

不论是机器代替体力劳动，或是计算机代替某种脑力劳动，其所以成为可能，关键在于所需代替的劳动已经“机械化”，也就是说已实现了刻板化或规格化. 正因为割麦、刈草、纺纱织布的动作已经是机械化刻板化了的，因而可据此造出割麦机、刈草机、纺纱机、织布机来. 也正因为加减乘除开方等运算这一类脑力劳动，几千年来就已经是机械刻板地进行，才有可能使得 17 世纪的法国数学家帕斯卡利用齿轮传动造出了第一台机械计算机 —— 加法机，并由莱布尼茨改进成为也能进行乘法的机器. 数学问题的机械化，就要求在运算或证明过程中，每前进一步之后，都有一个确定的、必须选择的下一步，这样沿着一条有规律的、刻板的道路，一直达到结论.

在中小学数学的范围里，就有着不少已经机械化了的课题. 除了四则、开方等运算外，解线性联立方程组就是一个很好的例子. 在中学用的数学课本中，往往介绍解线性方程组的各种“消去法”，其求解过程是一个按一定程序进行的计算过程，也就是一种机械的、刻板的过程. 根据这一过程编成程序，由电子计算机付诸实施，就可以不仅机器化而且达到自动化，在几分钟甚至几秒钟之内求出一个未知数多至上百个的线性方程组的解答来，这在手工计算几乎是不可能的. 如果用手工计算，即使是解只有三、四个未知数的方程组，也将是繁琐而令人厌烦的. 现代化的国防、经济建设中，大量出现的例如网络一类的问题，往往可归结为求解很多未

---

① 20 世纪 70,80 年代之交，我尝试用计算机证明几何定理取得成功，并由此提出了数学机械化的设想. 先后在一些通俗报告与写作中，解释数学机械化的意义与前景，例如 1978 年发表于《自然辩证法通讯》的《数学机械化问题》以及 1980 年发表于《百科知识》的《数学的机械化》. 两文都重载于 1995 年由山东教育出版社出版的《吴文俊论数学机械化》一书. 经过 20 多年众多学者的努力，数学机械化在各个方面都取得了丰富多彩的成就，并已出版了多种专著，汇集成现在的数学机械化丛书. 现据 1980 年的《百科知识》的“数学的机械化”一文，稍加修改并作增补，以代丛书前言.

知数的线性方程组. 这使得已经机械化了的线性方程解法在四个现代化中起着一种重要作用.

即使是不专门研究数学的人们, 也大都知道, 数学的脑力劳动有两种主要形式: 数值计算与定理证明 (或许还应包括公式推导, 但这终究是次要的). 著名的数理逻辑学家美国洛克菲勒大学教授王浩先生在一篇有名的《向机械化数学前进》的文章中, 曾列举了这两种数学脑力劳动的若干不同之点. 我们可以简略而概括地把它们对比一下:

计算	证明
易	难
繁	简
刻板	灵活
枯燥	美妙

计算, 如已经提到过的加减乘除开方与解线性方程组, 其所以虽繁而易, 根本原因正在于它已经机械化. 而证明的巧而难, 是大家都深有体会的, 其根本原因也正在于它并没有机械化. 例如, 我们在中学初等几何定理的证明中, 就经常要依靠诸如直观、洞察、经验, 以及其他一些模糊不清的原则, 去寻找捷径.

2. 从证明的机械化到机器证明

一个值得提出的问题是: 定理的证明是不是也能像计算那样机械化, 因而把巧而难的证明, 化为计算那样虽繁而易的劳动呢? 事实上, 这一证明机械化的设想, 并不始自今日, 它早就为 17 世纪时的大哲学家、大思想家和大数学家笛卡儿和莱布尼茨所具有, 只是直到 19 世纪末, 希尔伯特 (德国数学家, 1862～1943) 等创立并发展了数理逻辑, 这一设想才有了明确的数学形式, 又由于 20 世纪 40 年代电子计算机的出现, 才使这一设想的实现有了现实可能性.

从 20 世纪 20 、 30 年代以来, 数理逻辑学家们对于定理证明机械化的可能性, 进行了大量的理论探讨, 他们的结果大都是否定的. 例如哥德尔 (Gödel) 等的一条著名定理就说, 即使看来最简单的初等数论这一范围, 它的定理证明的机械化也是不可能的. 另一方面, 1950 年波兰数学家塔斯基 (Tarski) 则证明了初等几何 (以及初等代数) 这一范围的定理证明, 却是可以机械化的. 只是塔斯基的结果近于例外, 在初等几何及初等代数以外的大量结果都是反面的, 即机械化是不可能的. 1956 年以来美国开始了利用电子计算机做证明定理的尝试. 1959 年王浩先生设计了一个机械化方法, 用计算机证明了罗素等著的《数学原理》这一经典著作中的几百条定理, 只用了 9 分钟, 在数学与数理逻辑学界引起了轰动. 一时间, 机器证明的前景似乎非常乐观. 例如 1958 年时就有人曾经预测: 在 10 年之内计算机将

发现并证明一个重要的数学新定理. 还有人认为, 如果这样, 则不仅许多著名哲学家与数学家, 如皮亚诺、怀特海、罗素、希尔伯特以及图灵等人的梦想得以实现, 而且计算将成为科学的皇后, 人类的主人!

然而, 事情的发展却并不如预期那样美好. 尽管在 1976 年, 美国的哈肯等人, 在高速计算机上用了 1200 小时的计算时间, 解决了数学家们 100 多年来所未能解决的一个著名难题 —— 四色问题, 因此而轰动一时, 但是, 这只能说明计算机作为定理证明的辅助工具有着巨大潜力, 还不能认为这样的证明就是一种真正的机器证明. 用王浩先生的说法, 哈肯等关于四色定理的证明是一种使用计算机的特例机证, 它只适用于四色这一特殊的定理, 这与所谓基础机器证明之能适用于一类定理者有别. 后者才真正体现了机械化定理证明, 进而实现机器证明的实质. 另一面, 在真正的机械化证明方面, 虽然塔斯基在理论上早已证明了初等几何的定理证明是能机械化的, 还提出了据以造判定机也即是证明机的设想, 但实际上他的机械化方法非常繁, 繁到不可收拾, 因而远远不是切实可行的. 1976 年, 美国做了许多在计算机上证明定理的实验, 在塔斯基的初等几何范围内, 用计算机所能证明的只是一些近于同义反复的"儿戏式"的"定理". 因此, 有些专家曾经发出过这样悲观的论调: 如果专依靠机器, 则再过 100 年也未必能证明出多少有意义的新定理来.

3. 一条切实可行的道路

1976 年冬, 我们开始了定理证明机械化的研究. 1977 年春取得了初步成果, 证明初等几何主要一类定理的证明可以机械化. 在理论上说来, 我们的结果已包括在塔斯基的定理之中. 但与塔斯基的结果不同, 我们的机械化方法是切实可行的, 即使用手算, 依据机械化的方法逐步进行, 虽然繁复, 也可以证明一些艰深的定理.

我们的方法主要分两步, 第一步是引进坐标, 然后把需证定理中的假设与终结部分都用坐标间的代数关系来表示. 我们所考虑的定理局限于这些代数关系都是多项式等式关系的范围, 例如平行、垂直、相交、距离等关系都是如此. 这一步可以叫做几何的代数化. 第二步是通过代表假设的多项式关系把终结多项式中的坐标逐个消去, 如果消去的结果为零, 即表明定理正确, 否则再作进一步检查. 这一步完全是代数的, 即用多项式的消元法来验证.

上述两步都可以机械与刻板地进行. 根据我们的机械化方法编成程序, 以在计算机上实现机器证明, 并无实质上的困难. 事实上中国科学院数学研究所的某些同志以及国外的王浩先生都曾在计算机上试行过. 我们自己也曾在国产的长城 *203* 台式机上证明了像西摩松线那样不算简单的定理. 1978 年初我们又证明了初等微

分几何中主要的一类定理证明也可以机械化. 而且这种机械化方法也是切实可行的, 并据此用手算证明了不算简单的一些定理.

从我们的工作中可以看出, 定理的机械化证明, 往往极度繁复, 与通常既简且妙的证明形成对照, 这种以量的复杂来换取质的困难, 正是利用计算机所需要的.

在电子计算机如此发展的今天, 把我们的机械化方法在计算机上实现不仅不难, 而且有一台微型的台式机也就够了. 就像我们曾经使用过的长城 203, 它的存数最多只能到 234 个 10 进位的 12 位数, 就已能用以证明西摩松线那样的定理. 随着超大规模集成电路与其他技术的出现与改进, 微型机将愈来愈小型化而内存却愈来愈大, 功能愈来愈多, 自动化的程度也愈来愈高. 进入 21 世纪以后, 这一类方便的小型机器将为广大群众普遍使用. 它们不仅将成为证明一些不很简单的定理的武器, 而且还可用以发现并证明一些艰深的定理, 而这种定理的发现与证明, 在数学研究手工业式的过去, 将是不可想象的. 这里我们应该着重指出, 我们并不鼓励以后人们将使用计算机来证明甚至发现一些有趣的几何定理. 恰恰相反, 我们希望人们不再从事这种虽然有趣却即便是对数学甚至几何学本身也已意义不大的工作, 而把自己从这种工作中解放出来, 把自己的聪明才智与创造能力贯注到更有意义的脑力劳动上去.

还应该指出, 目前我们所能证明的定理, 局限于已经发现的机械化方法的范围, 例如初等几何与初等微分几何之内. 而如何超出与扩大这些机械化的范围, 则是今后需要长期探索的理论性工作.

4. 历史的启示与中国古代数学

我们发现几何定理证明的机械化方法是在 1976 至 1977 年之间. 约在两年之后, 我们发现早在 1899 年出版的希尔伯特的经典名著《几何基础》中, 就有着一条真正的正面的机械化定理: 初等几何中只涉及从属与平行关系的定理证明可以机械化. 当然, 原来的叙述并不是以机械化的语言来表达的, 也许就连希尔伯特本人也并没有对这一定理的机械化意义有明确的认识, 自然更不见得有其他人提到过这一定理的机械化内容. 希尔伯特是以公理化的典范而著称于世的, 但我认为, 该书更重要之处, 是在于提供了一条从公理化出发, 通过代数化以到达机械化的道路. 自然, 处于希尔伯特以及其后数学的一张纸一支笔的手工作业时代里, 公理化的思想与方法得到足够的重视与充分的发展, 而机械化的方向与意义受到数学家的忽视是完全可以理解的. 但在电子计算机已日益普及, 因而繁琐而重复的计算已成为不足道的现代, 机械化的思想应比公理化思想受到更大重视, 似乎是合乎实际的.

其次应该着重指出, 我们在从事机械化定理证明工作获得成果之前, 对塔斯基

的已有工作并无接触，更没有想到希尔伯特的《几何基础》会与机械化有任何关系．我们是在中国古代数学的启发之下提出问题并想出解决办法来的．

说起来道理也很简单：中国的古代数学基本上是一种机械化的数学．四则运算与开方的机械化算法由来已久．汉初完成的《九章算术》中，对开平方、开立方与解线性联立方程组的机械化过程，都有详细说明．宋代更发展到高次代数方程求数值解的机械化算法．

总之各个数学领域都有定理证明的问题，并不限于初等几何或微分几何．这种定理证明肇始于古希腊的欧几里得传统，现已成为近代纯粹数学或核心数学的主流．与之相异，中国的古代学者重视的是各种问题特别是来自实际要求的具体问题的解决．各种问题的已知数据与要求的数据之间，很自然地往往以多项式方程的形式出现．因之，多项式方程的求解问题，也就自然成为中国古代数学家研究的中心问题．从秦汉以来，所研究的方程由简到繁，不断有所前进，有所创新．到宋元时期，更出现了一个思想与方法的飞跃：天元术的创立．

"天元术"到元代朱世杰时又发展成四元术，所引入的天元、地元、人元、物元实际上相当于近代的未知元或未知数．将这些未知元作为通常的已知数那样加减乘除，就可得到与近代多项式和有理函数相当的概念与相应的表达形式和运算法则．一些几何性质与关系很容易转化成这种多项式或有理函数的形式及其关系．这使得过去依题意列方程这种无法可循需要高度技巧的工作从此变得轻而易举．朱世杰 1303 年的《四元玉鉴》又给出了解任意多至四个未知元的多项式方程组的方法．这里限于 4 个未知元只是由于所使用的计算工具（算筹和算板）的限制．实质上他解方程的思想路线与方法完全可以适用于任意多的未知元．

不问可知，在当时的具体条件下，朱世杰的方法有许多缺陷．首先，当时还没有复数的概念，因此朱世杰往往限于求出（正）实值．这无可厚非，甚至在 17 世纪 Descartes 的时代也还往往如此．但此外朱世杰在方法上也未臻完善．尽管如此，朱世杰的思想路线与方法步骤是完全正确的，我们在上世纪 70 年代之末，遵循朱世杰的思想与方法的基本实质，采用美国数学家 J.F.Ritt 在 1935, 1950 年关于微分方程代数研究书中所提供的某些技术，得出了解任意复多项式方程组的一般算法，并给出了全部复数解的具体表达形式．此后又得出了实系数时求实解的方法，为重要的优化问题提供了一个具体的方法．

由于多种问题往往自然导致多项式方程组的求解，因而我们解方程的一般方法可被应用于形形色色的问题．这些问题可以来自数学自身，也可以来自其他自然科学或工程技术．在本丛书的第一本吴文俊的《数学机械化》一书中，可以看到这些应用的实例．工程技术方面的应用，在本丛书中有高小山的《几何自动作图与智能 CAD》与陈发来和冯玉瑜的《代数曲面造型》两本专著．上述解多项

式方程组的一般方法已推广至代微分方程的情形. 许多应用以及相应论著正在酝酿之中.

5. 未来的技术革命与时代的使命

宋元时代天元术与四元术的创造, 把许多问题特别是几何问题转化成代数方程与方程组的求解问题. 这一方法用于几何可称为几何的代数化. 12 世纪的刘益将新法与"古法"比较, 称"省功数倍". 这可以说是减轻脑力劳动使数学走上机械化道路的一项伟大的成就.

与天元术的创造相伴, 宋元时代的数学又引进了相当于现代多项式的概念, 建立了多项式的运算法则和消元法的有关代数工具, 使几何代数化的方法得到了系统的发展, 这些可见于宋元时代幸以保存至今的杨辉、李冶、朱世杰的许多著作之中. 几何的代数化是解析几何的前身, 这些创造使我国古代数学达到了又一个高峰. 可以说, 当时我国已到达了解析几何与微积分的大门, 具备了创立这些数学关键领域的条件, 但是各种原因使我们数学的雄伟步伐就在这些大门之前停顿下来. 几百年的停顿, 使我们这个古代的数学大国在近代变成了数学上的纯粹入超国家. 然而, 我国古代机械化与代数化的光辉思想和伟大成就是无法磨灭的. 本人关于数学机械化的研究工作, 就是在这些思想与成就启发之下的产物, 它是我国自《九章算术》以迄宋元时期数学的直接继承.

恩格斯曾经指出, 枪炮的出现消除了体力上的差别, 使中世纪的骑士阶级从此销声匿迹, 为欧洲从封建时代进入到资本主义时代准备了条件. 近年有些计算机科学家指出, 个人用计算机的出现, 其冲击作用可与枪炮的出现相比. 枪炮使人们在体力上难分强弱, 而个人用计算机将使人们在智力上难分聪明愚鲁. 又有人对数学的未来提出看法, 认为计算机的出现, 将使数学现在一张纸一支笔的方法, 在历史的长河中, 无异于石器时代的手工方法. 今天的数学家们, 不得不面对计算机的挑战, 但是, 也不必妄自菲薄. 大量繁复的事情交给计算机去做了, 人脑将仍然从事富有创造性的劳动.

我国在体力劳动的机械化革命中曾经掉队, 以致造成现在的落后状态. 在当前新的一场脑力劳动的机械化革命中, 我们不能重蹈覆辙. 数学是一种典型的脑力劳动, 它的机械化有着许多其他类型脑力劳动所不及的有利条件. 它的发扬与实现对我国的数学家是一种时代的使命. 我国古代数学的光辉, 都鼓舞着我们为实现数学的机械化, 在某种意义上也可以说是真正的现代化而勇往直前.

吴文俊

2002 年 6 月于北京

前言

实域理论的发展应追溯到著名的 Hilbert 第十七问题. 根据第十七问题的特有形式, E. Artin 和 O. Schreier 洞察到实数域及其子域的最本质的属性, 这些属性包括两个方面: 一是与平方和相关的 "实性"; 二是与运算相适应的元素之间大小关系即 "序" 关系. E. Artin 和 O. Schreier 把这些本质属性引进到域范畴中, 由此建立了著名的 Artin–Schreier 理论, 这一理论是实域理论的基石. 正是基于他和 O. Schreier 所建立的理论, Artin 肯定地解答了 Hilbert 第十七问题, 这使得 Artin 进入 Hilbert 问题解答者的光荣行列中.

由于实域具有相当的普遍性, 且其理论和方法的适用性也颇为广泛, 从而自 Artin 以来, 有关实域的研究一直深入开展, 由此逐渐发展成 "实域论" 这门独特的数学分支. 实域理论不仅是一门自成体系的学科, 同时也是当前正在日益发展的实代数几何的基础. 从数学机械化的发展趋势来看, 代数闭域上代数方程组的求解以及等式型几何命题的自动推理已获丰硕成果, 而实代数方程组的求解以及不等式(包括不等式型几何命题) 的研究正方兴未艾. 与前者相比, 后者的研究特点正好体现在 "实性" 和 "序" 两个方面. 从而, 实代数方程组的求解以及不等式的研究必然涉及到实域理论中的有关概念、方法和结果. 因此, 对于从事实代数几何和构造性实代数几何方面研究工作的人们来说, 了解实域的有关理论和方法是必要的.

本书力图较全面地介绍实域理论在各个方面的发展, 使读者在兴趣之余有能力进一步阅读有关文献. 为方便读者更进一步了解实域理论的有关内容, 书末列出了大量参考文献以飨读者. 本书要求读者具备抽象代数和一般的域论知识. 限于作者的学识水平, 遗漏与谬误在所难免, 敬请读者不吝指正.

作者是在戴执中先生的指引下, 才得以迈进实域理论和实代数几何这一领域. 在此, 谨向戴执中先生致以衷心谢意. 作者感谢吴文俊院士以及高小山研究员为首席专家的国家九七三项目 "数学机械化与自动推理平台" 专家委员会, 正是由于他们的关照和支持, 作者才有幸成为项目组成员, 且本书被接纳于数学机械化丛书之中. 还应该感谢曾苹同志, 她为书稿的打印付出了辛勤的劳动.

作 者

于南昌

常用记号一览表

$\mathbb{N}$	自然数集
$\mathbb{Z}$	整数集 (环)
$\mathbb{Q}$	有理数域
$\mathbb{R}$	实数域
$A \setminus B$	集合B在集合A中的补集
$A \times B$	集合A和集合B的笛卡儿积
A^n	集合A的n重 (笛卡儿) 幂集
$\dot{T}$	环 (或域) 的子集T中全体非零元组成的集合
$[K:F]$	域扩张K/F的扩张次数
$[G:H]$	子群H在群G中的指标
$\|G\|$	群G的阶
$\deg f(x)$	单元多项式$f(x)$的次数
$f'(x)$	单元多项式$f(x)$的微商 (导数)
$\deg(f;x)$	多元多项式f关于变元x的次数
$\dfrac{\partial f}{\partial x}$	多元多项式f关于变元x的偏导数
$\mathrm{Res}(f,g;x)$	多项式f和g关于变元x的结式
A^{T}	矩阵A的转置矩阵

目　录

第一章　实域和序域

本章主要介绍域的“实性”、“序”与“亚序”等基本概念，同时研究它们之间的相互关系. 作为序与域扩张的两者结合，我们讨论序在域扩张上可拓展的充要条件. 此外，我们对一个域的全体序组成的集合赋予拓扑结构，使之成为一个拓扑空间 —— 序空间.

§1.1　实域、序和亚序

设 F 是一个域，其中零元和单位元分别记作 0 和 1. 对此，我们可构造 F 的如下非空子集:

$$S_F := \left\{ \text{有限和} \sum_{i=1}^{m} x_i^2 \middle| x_i \in F, i = 1, \cdots, m \right\}.$$

定义 1.1.1　一个域 F 称作形式实域 (或简称实域), 若 $-1 \notin S_F$.

显然，实数域 $\mathbb{R}$ 是实域，且一个实域的所有子域都是实域. 此外，实域的特征必为零. 事实上，如若域 F 的特征为素数 p, 则有 $-1 = 1^2 + \cdots + 1^2 (p-1$ 项) $\in S_F$. 因此，我们可认定：有理数域 $\mathbb{Q}$ 包含在每个实域之中.

为表达上的方便，对于域 F 的任意子集 T, 我们引入如下记号:

$$-T = \{-a \mid a \in T\};$$

$$T + T = \{a + b \mid a, b \in T\};$$

$$T \cdot T = \{ab \mid a, b \in T\}.$$

定义 1.1.2　设 P 是域 F 的一个子集. 若下列条件成立:

(1) $P \neq F$;

(2) $F = P \cup -P$;

(3) $P + P \subseteq P$, 且 $P \cdot P \subseteq P$,

则称 P 是 F 的一个正锥.

注　(1) 当 P 是域 F 的正锥时，显然有 $0, 1 \in P$, 而 $-1 \notin P$. 此时还有 $P \cap -P = \{0\}$; 否则，有非零 $a \in P \cap -P$. 从而对于任意 $x \in F$, 当 $xa^{-1} \in P$ 时，$x = (xa^{-1})a \in P \cdot P \subseteq P$; 当 $xa^{-1} \in -P$ 时，$x = (xa^{-1})a \in (-P) \cdot (-P) \subseteq P$, 这导致矛盾：$F = P$. 此外易知，对于每个 $x \in F$, $x^2 \in P$.

(2) 若 P_1 和 P_2 都是域 F 的正锥，且 $P_1 \subseteq P_2$, 则 $P_1 = P_2$. 事实上，如若不然，则有 $a \in P_2$ 但 $a \notin P_1$. 从而 $a \in -P_1 \subseteq -P_2$. 于是 $a \in P_2 \cap -P_2 = \{0\}$, 即

$a=0\in P_1$, 矛盾.

定义 1.1.3 域 F 中元素之间的一个二元关系 $\leqslant$ 称作 F 的一个序, 如果下列条件成立:

(1) 对于任意 $a\in F$, $a\leqslant a$;

(2) 若 $a\leqslant b$ 且 $b\leqslant a$, 则 $a=b$;

(3) 若 $a\leqslant b$ 且 $b\leqslant c$, 则 $a\leqslant c$;

(4) 对于任意 $a, b\in F$, $a\leqslant b$ 或者 $b\leqslant a$;

(5) 若 $a\leqslant b$, 则对于任意 $c\in F$, $a+c\leqslant b+c$;

(6) 若 $0\leqslant a$ 且 $0\leqslant b$, 则 $0\leqslant ab$.

"正锥" 和 "序" 这两个概念在表述方面尽管迥然不同, 但它们之间可互相转化. 事实上, 对于域 F 的一个序 $\leqslant$, 集合 $P_{\leqslant}:=\{a\in F\mid 0\leqslant a\}$ 是 F 的一个正锥. 反过来, 对于域 F 的一个正锥 P, 我们可按如次方式规定 F 上的一个二元关系 $\leqslant_P$: 对于 $a, b\in F$, $a\leqslant_P b$ 当且仅当 $b-a\in P$. 容易验证: $\leqslant_P$ 是域 F 的一个序. 进一步可知, $P_{\leqslant_P}=P$, 且 $\leqslant_{P_{\leqslant}}=\leqslant$. 正因为这一缘故, 有时我们不加区别地把 "正锥" 也称作 "序".

如果 $\leqslant$(或 P) 是域 F 的一个序 (或正锥), 那么我们将迳称 $(F,\leqslant)$(或 (F,P)) 是一个序域 . 对于域 F 的一个序 $\leqslant$ 以及 $a, b\in F$, 若 $a\leqslant b$ 但 $a\neq b$, 则习惯地记作 $a<b$. 此时, 域 F 中一个元素 a 称作正元素, 如果 $0<a$, 这等价于: a 是 $P_{\leqslant}$ 中的非零元素, 其中 $P_{\leqslant}$ 为 $\leqslant$ 的对应正锥.

例 1 设 $\mathbb{R}$ 为实数域, 且记 $\mathbb{R}^2=\{a^2\mid a\in\mathbb{R}\}$. 容易验证, $\mathbb{R}^2$ 是 $\mathbb{R}$ 的一个正锥, 且 $\mathbb{R}^2$ 的对应序为实数之间通常的大小关系.

例 2 设 $\mathbb{Q}$ 为有理数域, 且 $\mathbb{Q}^+$ 为所有非负有理数组成的集合, 则 $\mathbb{Q}^+$ 是 $\mathbb{Q}$ 的一个正锥, 且 $\mathbb{Q}^+$ 的对应序为通常的有理数之间大小关系.

例 3 设 (F,P) 是一个序域, t 是域 F 上一个未定元, 构造域 $F(t)$ 的如下子集:

$$P_{0+}:=\{0\}\cup\left\{\frac{f(t)}{g(t)}\middle| f(t),\, g(t)\in F[t], \text{且} f(t)g(t) \text{的尾项系数属于} P\right\}.$$

容易验证: P_{0+} 是 $F(t)$ 的一个正锥.

此外, 我们还可以构造域 $F(t)$ 的如下子集:

$$P_{+\infty}:=\{0\}\cup\left\{\frac{f(t)}{g(t)}\middle| f(t),\, g(t)\in F[t], \text{且} f(t)g(t) \text{的首项系数属于} P\right\}.$$

同样可验证: $P_{+\infty}$ 是 $F(t)$ 的一个正锥.

自然会提出这样一个问题：怎样的域才具有序 (正锥)? 问题的解答与“实域”这一概念紧密相连. 为使解答的问题更具普遍意义，我们给出下面的定义：

定义 1.1.4 设 T 是域 F 的一个子集，若下列条件成立：

(1) $T+T\subseteq T$ 且 $T\cdot T\subseteq T$;

(2) 对于任意 $a\in F$, $a^2\in T$;

(3) $-1\notin T$,

则称 T 是域 F 的一个亚正锥 (或亚序). 此时，亦称 (F,T) 是一个亚序域.

显然，正锥必为亚正锥. 易知，对于一个域 F, S_F 是 F 的一个亚正锥，当且仅当 $-1\notin S_F$, 即 F 是一个实域. 若域 F 有一个亚序 T, 则由定义 1.1.4 中条件 (1) 和 (2) 知，$S_F\subseteq T$. 从而由条件 (3) 可知，$-1\notin S_F$. 这表明：F 是一个实域. 此时，显然 F 的每个亚正锥都包含 S_F, 从而我们称 S_F 为实域 F 的弱亚正锥 (或弱亚序).

设 T 是域 F 的一个亚序，$t\in T$ 且 $t\neq 0$, 则 $t^{-1}=(t^{-1})^2t\in T\cdot T\subseteq T$. 这表明：$T$ 中全部非零元素对于 F 的乘法组成一个群.

引理 1.1.1 设 T 是域 F 的一个亚正锥. 若 $a\in F$ 但 $-a\notin T$, 则 $T+Ta:=\{t_1+t_2a\mid t_1,t_2\in T\}$ 为 F 的一个包含 T 的亚正锥.

证明 显然，$T\subseteq T+Ta$ 且 $T+Ta$ 满足定义 1.1.4 中条件 (1) 和 (2). 假若 $-1\in T+Ta$, 则对于某两个 $t_1,t_2\in T$, $-1=t_1+t_2a$. 由于 $-1\notin T$, 从而 $t_2\neq 0$. 由上面的讨论知，$t_2^{-1}\in T$. 由此有，$-a=t_2^{-1}(1+t_1)\in T\cdot T\subseteq T$, 与所设矛盾. 因而，$-1\notin T+Ta$. 因此，$T+Ta$ 为 F 的一个亚序. 证毕.

由引理 1.1.1 , 容易证明下面的重要定理：

定理 1.1.2 设 T 是域 F 的一个亚正锥，且记 $\mathcal{X}_F(T)$ 为域 F 的所有包含 T 的正锥组成的集合，则

$$T=\bigcap_{P\in\mathcal{X}_F(T)}P.$$

证明 显然，$T\subseteq\bigcap_{P\in\mathcal{X}_F(T)}P$. 设 $a\in F$, 但 $a\notin T$, 则由引理 1.1.1 知，$T_1:=T+T(-a)$ 是 F 的一个亚正锥. 作如下集合

$$\Xi:=\{S\mid S\text{ 是 }F\text{ 的亚正锥，使得 }T_1\subseteq S\}.$$

显然，$T_1\in\Xi$, 且 Ξ 对于集合包含关系 $\subseteq$ 是一个偏序集. 设 $\{S_\lambda\mid\lambda\in\Lambda\}$ 是 Ξ 中任意链 (全序子集), 其中 Λ 是指标集. 令 $S=\bigcup_{\lambda\in\Lambda}S_\lambda$. 易知，$S\in\Xi$, 且 S 显然为链 $\{S_\lambda\mid\lambda\in\Lambda\}$ 的一个上界. 由 Zorn 引理，Ξ 中有一个极大元 P_1. 此时，我们可断定：P_1 是 F 的一个正锥. 事实上，P_1 显然满足定义 1.1.2 中条件 (3). 此外,

由于 $-1 \notin P_1$, 从而 P_1 满足定义 1.1.2 中条件 (1). 现设 $b \in F$ 但 $b \notin P_1$, 则由引理 1.1.1 知, $P_1 + P_1(-b)$ 是包含 P_1 的一个亚正锥. 显然, $P_1 + P_1(-b) \in \Xi$. 由 P_1 的极大性, $P_1 + P_1(-b) = P_1$. 从而, $-b \in P_1$ 即 $b \in -P_1$. 因而, $F \subseteq P_1 \cup -P_1$. 必然 $F = P_1 \cup -P_1$, 即 P_1 满足定义 1.1.2 中条件 (2). 因此, $P_1 \in \mathcal{X}_F(T)$.

注意到, $-a \in T_1 \subseteq P_1$, 即 $a \in -P_1$. 从而 $a \notin P_1$; 否则 $a \in P_1 \cap -P_1 = \{0\}$, 即 $a = 0 \in T$, 矛盾. 这样, 我们有 $a \notin \bigcap\limits_{P \in \mathcal{X}_F(T)} P$. 这表明: $\bigcap\limits_{P \in \mathcal{X}_F(T)} P \subseteq T$. 从而定理获证.

推论 若 T 是域 F 的一个亚正锥, 则 F 至少有一个正锥 P, 使得 $T \subseteq P$.

设 (F,T) 是一个亚序域. 域 F 的一个正锥 P 称作 (F,T) 的一个正锥, 若 $T \subseteq P$. 自然, 域 F 的一个序 $\leqslant$ 称作 (F,T) 的一个序, 若 $\leqslant$ 的对应正锥 $P_{\leqslant}$ 是 (F,T) 的一个正锥. 因此, 定理 1.1.2 表明: 亚序域 (F,T) 的所有正锥的交集恰好为亚正锥 T.

现在, 我们容易建立下面的定理, 这一定理回答了上面所提到的问题.

定理 1.1.3 对于一个域 F, 下列叙述是等价的:

(1) F 是一个实域;

(2) F 的特征不为 2, 且 $F \neq S_F$;

(3) F 至少有一个序 (正锥).

证明 (1) $\Longrightarrow$ (2): 显然.

(2) $\Longrightarrow$ (3): 显然, $S_F + S_F \subseteq S_F$, $S_F \cdot S_F \subseteq S_F$, 且对于每个 $a \in F$, 有 $a^2 \in S_F$. 假设 $-1 \in S_F$, 则 $-1 = \sum\limits_{i=1}^{m} a_i^2$, 这里 m 为自然数, $a_i \in F$, $i = 1, \cdots, m$. 由于 F 的特征不为 2, 从而对于每个 $a \in F$, 有 $a = \left(\frac{a+1}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2 = \left(\frac{a+1}{2}\right)^2 + \sum\limits_{i=1}^{m} a_i^2 \left(\frac{a-1}{2}\right)^2 \in S_F$. 这导致出矛盾: $F = S_F$. 因而 $-1 \notin S_F$, 即 S_F 是 F 的一个亚正锥. 根据上面推论, F 至少有一个正锥 (包含 S_F).

(3) $\Longrightarrow$ (1): 设 F 有一个正锥 P. 由于 P 也是 F 的亚正锥, 从而由上面讨论知, F 是一个实域. 证毕.

定理 1.1.4 设 F 是一个特征不为 2 的域, 且记 $\mathcal{X}_F$ 为域 F 的所有正锥组成的集合, 则

$$S_F = \bigcap_{P \in \mathcal{X}_F} P.$$

证明 当 F 不是实域时, 由定理 1.1.3 知, $S_F = F$. 此时, 由上面讨论知, $\mathcal{X}_F = \phi$. 于是 $S_F = \bigcap\limits_{P \in \mathcal{X}_F} P$.

当 F 是实域时, S_F 是 F 的一个亚正锥. 注意到, $\mathcal{X}_F(S_F) = \mathcal{X}_F$. 从而由定

理 1.1.2 知，上面结论中的等式成立．证毕．

推论 设 F 是一个实域，则 F 有惟一序，当且仅当 S_F 是 F 的正锥．

证明 设 P 是 F 的惟一正锥，则由定理 1.1.4 有， $S_F = P$. 反过来，设 S_F 是 F 的正锥，且 P 是 F 的任意正锥，则必有 $S_F \subseteq P$. 由定义 1.1.2 后的注 (2), $P = S_F$. 证毕．

域 F 中元素 a 称作全正元，若对于 F 的每个序 $\leqslant$, 都有 $0 < a$. 定理 1.1.4 表明：当 F 的特征 $\neq 2$ 时， F 中所有全正元恰好是 S_F 中全部非零元．

§1.2 序域的区间拓扑

设 (F, P) 是一个序域， $\leqslant$ 是 P 的对应序．正如实数域一样，我们可以在 F 上规定所谓的“区间拓扑”. 设 $a, b \in F$, 且 $a < b$, 则可规定 F 的如下子集：

$$]a, b[:= \{x \in F \mid a < x < b\}.$$

显然， $\frac{1}{2}(a+b) \in]a, b[$. 如上非空子集 $]a, b[$ 称作左和右端点分别为 a 和 b 的开区间．容易验证，诸如 $]a, b[$ 的所有开区间组成 F 的一个开集基．此时，由这些开区间所诱导的拓扑称作域 F 的由 P (或 $\leqslant$) 所诱导的区间拓扑，或序域 (F, P) 的区间拓扑．

同时，对于任意 $x \in F$, 可规定 $|x|_P = x$, 若 $x \in P$, 或 $|x|_P = -x$, 若 $x \in -P$. 此外，我们称 $|x|_P$ 为元素 x 关于 P (或 $\leqslant$) 的绝对值．容易验证，所规定的绝对值具有通常绝对值的有关性质： (1) 对于 $x \in F$, $0 \leqslant |x|_P = |-x|_P$; (2) 对于 $x, y \in F$, $|x|_P - |y|_P \leqslant |x \pm y|_P \leqslant |x|_P + |y|_P$, 且 $|xy|_P = |x|_P |y|_P$. 为简便起见，在所给的正锥 P 明确而不致混淆的情况下，元素 x 关于 P (或 $\leqslant_P$) 的绝对值可简记作 $|x|$.

对于 $a, \delta \in F$, 其中 $\delta > 0$, 可规定 F 的如下子集：

$$\mathcal{O}(a; \delta) = \{x \in F \mid |x - a|_P < \delta\},$$

且称如上子集 $\mathcal{O}(a; \delta)$ 为中心为 a, 半径为 δ 的开区间．显然，我们有

$$]a, b[= \mathcal{O}(\frac{a+b}{2}; \frac{b-a}{2}),$$

而

$$\mathcal{O}(a; \delta) =]a - \delta, a + \delta[.$$

对于序域 (F, P) 的区间拓扑， F 上 n 维线性空间 F^n 可看作 F 的乘积拓扑空间．为叙述方便起见，这样的乘积拓扑称作由 P (或 $\leqslant$) 诱导的乘积区间拓扑．

命题 1.2.1 设 $(F, \leqslant)$ 是一个序域，则下列映射是连续的：

(1) $F\times F$ 到 F 的加法映射 $+$: $(x,y)\mapsto x+y$;

(2) F 到 F 的求负元映射 $-$: $x\mapsto -x$;

(3) $F\times F$ 到 F 的乘法映射 $\times$: $(x,y)\mapsto xy$;

(4) F^* 到 F 的求逆元映射 $()^{-1}$: $x\mapsto x^{-1}$, 这里 $F\times F$ 被赋予由 $\leqslant$ 诱导的乘积区间拓扑, F^* 是 F 关于区间拓扑的子空间.

证明 (1) 设 $a,\ b\in F$, 且 $a+b\in\mathcal{O}(d,\epsilon)$, 其中 $d,\ \epsilon\in F$ 且 $\epsilon>0$. 令 $\epsilon_1=\min\{d+\epsilon-a-b,-d+\epsilon+a+b\}$, 则 $\epsilon_1\in F$, $\epsilon_1>0$ 且 $\mathcal{O}(a+b,\epsilon_1)\subseteq\mathcal{O}(d,\epsilon)$. 再令 $\delta=\dfrac{1}{2}\epsilon_1$. 易知, 对于任意 $(x,y)\in\mathcal{O}(a,\delta)\times\mathcal{O}(b,\delta)$, $x+y\in\mathcal{O}(a+b,\epsilon_1)\subseteq\mathcal{O}(d,\epsilon)$. 这表明: 加法映射是连续的.

(2) 设 $a\in F$, 且 $-a\in\mathcal{O}(d,\epsilon)$, 其中 $d,\ \epsilon\in F$ 且 $\epsilon>0$. 此时易知, $a\in\mathcal{O}(-d,\epsilon)$, 且对于任意 $x\in\mathcal{O}(-d,\epsilon)$, $-x\in\mathcal{O}(d,\epsilon)$. 因此, 求负元映射是连续的.

(3) 设 $a,\ b\in F$, 且 $ab\in\mathcal{O}(d,\epsilon)$, 其中 $d,\ \epsilon\in F$ 且 $\epsilon>0$. 同样令 $\epsilon_1=\min\{d+\epsilon-ab,-d+\epsilon+ab\}$, 则 $\epsilon_1\in F$, $\epsilon_1>0$ 且 $\mathcal{O}(ab,\epsilon_1)\subseteq\mathcal{O}(d,\epsilon)$. 令 $\delta_1=\dfrac{\epsilon_1}{1+2b^2}$, $\delta_2=\dfrac{\epsilon_1}{2|a|+2\delta_1}$, 则对于任意 $(x,y)\in\mathcal{O}(a,\delta_1)\times\mathcal{O}(b,\delta_2)$, $|xy-ab|=|(x-a)b+x(y-b)|\leqslant\delta_1|b|+|x|\delta_2\leqslant\dfrac{|b|\epsilon_1}{1+2b^2}+(|a|+\delta_1)\cdot\dfrac{\epsilon_1}{2|a|+2\delta_1}<\dfrac{\epsilon_1}{2}+\dfrac{\epsilon_1}{2}=\epsilon_1$, 即 $xy\in\mathcal{O}(ab,\epsilon_1)\subseteq\mathcal{O}(d,\epsilon)$. 这表明乘法映射是连续的.

(4) 设 $a\in F$, 且 $a^{-1}\in\mathcal{O}(d,\epsilon)$, 其中 $d,\ \epsilon\in F$ 且 $\epsilon>0$. 由于 $\mathcal{O}(d,\epsilon)$ 是一个开集, 从而有正元素 $\epsilon_1\in F$, 使得 $\mathcal{O}(a^{-1},\epsilon_1)\subseteq\mathcal{O}(d,\epsilon)$. 令 $\delta=\min\left\{\dfrac{|a|}{2},\dfrac{a^2\epsilon_1}{2}\right\}$, 则对于任意 $x\in\mathcal{O}(a,\delta)$, $|x|\geqslant|a|-|a-x|>|a|-\delta\geqslant|a|-\dfrac{|a|}{2}=\dfrac{|a|}{2}$, 进而有 $|x^{-1}-a^{-1}|=\dfrac{|x-a|}{|xa|}<\dfrac{2\delta}{a^2}\leqslant\epsilon_1$. 于是 $x^{-1}\in\mathcal{O}(a^{-1},\epsilon_1)\subseteq\mathcal{O}(d,\epsilon)$. 这表明求逆元映射是连续的. 证毕.

对于域 F 上的一个拓扑 $\mathcal{T}$, 若加法映射 $+$, 求负元映射 $-$, 乘法映射 $\times$ 和求逆元映射 $()^{-1}$ 都是连续的, 则称 F 是一个关于 $\mathcal{T}$ 的拓扑域. 因此, 命题 1.2.1 表明: 一个域对于由序所诱导的区间拓扑是拓扑域. 设 $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$, 其中 $F[x_1,\cdots,x_n]$ 是域 F 上含未定元 $x_1,\ \cdots,\ x_n$ 的 n 元多项式环, 则我们有从 F^n 到 F 的一个多项式映射 f: $(a_1,\cdots,a_n)\mapsto f(a_1,\cdots,a_n)$. 注意到, 多项式映射可表示为加法映射, 求负元映射和乘法映射的一个复合映射. 因此, 对于一个关于 $\mathcal{T}$ 的拓扑域 F, 任意一个多项式映射都是连续的. 这样, 由命题 1.2.1 立即有如下推论.

推论 1 设 (F,P) 是一个序域, 且 $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$, 则 F^n 到 F 的多项式映射 f 是连续的, 这里 F 被赋予由 P 诱导的区间拓扑, F^n 被赋予相应的乘积拓扑.

推论 2 设 $(F,\leqslant)$ 是一个序域，且 $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$. 若 $a_1,\cdots,a_n\in F$, 使得 $f(a_1,\cdots,a_n)>0$, 则存在正元素 $\delta\in F$, 使得 $f(x_1,\cdots,x_n)>0$, 只要 $|x_i-a_i|<\delta$, $i=1,\cdots,n$.

证明 令 $\epsilon=f(a_1,\cdots,a_n)$. 由推论 1 可知，有正元素 $\delta_1,\cdots,\delta_n\in F$, 使得对于任意 $(x_1,\cdots,x_n)\in\mathcal{O}(a_1,\delta_1)\times\cdots\times\mathcal{O}(a_n,\delta_n)$, $f(x_1,\cdots,x_n)\in\mathcal{O}(f(a_1,\cdots,a_n),\epsilon)$. 此时有 $f(x_1,\cdots,x_n)=(f(x_1,\cdots,x_n)-f(a_1,\cdots,a_n))+f(a_1,\cdots,a_n)>-\epsilon+f(a_1,\cdots,a_n)=0$. 从而 $\delta=\min\{\delta_1,\cdots,\delta_n\}$ 为所求. 证毕.

引理 1.2.2 设 K 是实域 F 的一个扩张， $\alpha\in K$ 是域 F 上的代数元，则有 $M\in S_F$, 使得对于 K 的每个序 $\leqslant$, 均有 $|\alpha|<M$.

证明 设 α 在域 F 上的极小多项式为

$$x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,$$

其中 $a_0,a_1,\cdots,a_{n-1}\in F$.

令 $M=\frac{1}{2}(n+1+a_0^2+a_1^2+\cdots+a_{n-1}^2)\in S_F$. 假若对于 K 的某个序 $\leqslant$, $|\alpha|\geqslant M$, 则 $|\alpha|>1$, 且 $0=|\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0|\geqslant|\alpha^n|-|a_{n-1}\alpha^{n-1}|-\cdots-|a_1\alpha|-|a_0|\geqslant|\alpha^n|-(|a_0|+|a_1|+\cdots+|a_{n-1}|)|\alpha^{n-1}|$. 由此有 $|\alpha|\leqslant|a_0|+|a_1|+\cdots+|a_{n-1}|=M-\frac{1}{2}[1+(1-|a_0|)^2+(1-|a_1|)^2+\cdots+(1-|a_{n-1}|)^2]<M$, 矛盾. 因此，对于 K 的每个序 $\leqslant$, $|\alpha|<M$. 证毕.

实际上，由上面的证明，我们可以建立如下命题.

命题 1.2.3 设 F 是一个实域， $f(x)\in F[x]$ 是一个非零多项式，则有 $M\in S_F$, 使得对于 F 的任意扩张 K 的每个序 $\leqslant$, $|\alpha|<M$, 只要 $\alpha\in K$, 且 $f(\alpha)=0$.

根据上面引理，我们容易证明下面的命题.

命题 1.2.4 设 $(K,\leqslant)$ 是一个序域， F 为 K 的一个子域，使得 K 是 F 的代数扩张，则如下开区间

$$\mathcal{O}(y,\delta),\ \text{其中}\ y\in K,\ \delta\in S_F,\ \text{且}\ \delta\neq 0,$$

组成 $(K,\leqslant)$ 的区间拓扑的一个基.

证明 由于如上开区间对于 $(K,\leqslant)$ 的区间拓扑是开子集，从而只须证明：对于任意 $y\in\mathcal{O}(\alpha,\epsilon)$, 其中 $\alpha,\epsilon\in K$ 且 $\epsilon>0$, 有 $\delta\in S_F$, 使得 $\mathcal{O}(y,\delta)\subseteq\mathcal{O}(\alpha,\epsilon)$. 事实上，由于 $\mathcal{O}(\alpha,\epsilon)$ 是开子集，从而有某个正元素 $\epsilon_1\in K$, 使得 $\mathcal{O}(y,\epsilon_1)\subseteq\mathcal{O}(\alpha,\epsilon)$. 注意到， ϵ_1^{-1} 是 F 上代数元. 由引理 1.2.2 知，有 $M\in S_F$, 使得 $|\epsilon_1^{-1}|<M$, 即 $\epsilon_1>\frac{1}{M}$. 令 $\delta=\frac{1}{M}\in S_F$, 则有 $\mathcal{O}(y,\delta)\subseteq\mathcal{O}(y,\epsilon_1)\subseteq\mathcal{O}(\alpha,\epsilon)$. 证毕.

§1.3 序的扩张

设 K 是域 F 的一个扩张. 若 Q 是 K 的一个正锥, 易知 $Q\cap F$ 是 F 的一个正锥. 设 P 是域 F 的一个正锥, Q 是域 K 的正锥. 若 $P\subseteq Q$, 则称 Q 是正锥 P 在 K 上的一个序拓展. 此时, 亦称 (K,Q) 是序域 (F,P) 的一个序扩张. 根据定义 1.1.2 后面的注 (2), 若 Q 是正锥 P 在 K 上的一个序拓展, 则必有 $Q\cap F=P$. 更一般地, 若 T,S 分别为 F 和 K 的亚正锥, 使得 $T\subseteq S$, 则称 S 是亚序 T 在 K 上的一个拓展, 或称 (K,S) 是亚序域 (F,T) 的一个扩张. 对于亚序域 (F,T), F 的一个扩张 K 称作 (F,T) 的一个实扩张, 若亚序 T 在 K 上有一个拓展. 根据定理 1.1.2 的推论可知, K 是亚序域 (F,T) 的一个实扩张, 当且仅当 K 有一个正锥 Q, 使得 $T\subseteq Q$. 特别地, 称 K 是域 F 的一个实扩张, 若 K 是 (F,S_F) 的一个实扩张, 其中 S_F 是域 F 的弱亚正锥. 显然, K 是域 F 的一个实扩张, 当且仅当 K 是一个实域.

设 (F,T) 是一个亚序域, K 是 F 的一个扩张, 则可构造 K 的如下子集:

$$S_K(T):=\left\{\sum_{i=1}^{n}t_i\alpha_i^2 \mid n\text{为自然数}, t_i\in T, \alpha_i\in K, i=1,\cdots,n\right\}.$$

容易证明, $T\subseteq S_K(T)$, $S_K(T)$ 对于 K 的加法和乘法是封闭的, 且 $S_K(T)$ 中全部非零元素对于 K 的乘法组成一个群.

定理 1.3.1 设 (F,T) 是一个亚序域, K 是 F 的一个扩张, 则下列叙述等价:

(1) T 在 K 上有一个拓展, 即 K 是 (F,T) 的实扩张;

(2) $-1\notin S_K(T)$;

(3) K 有一个正锥 Q, 使得 $T\subseteq Q$.

证明 (1) $\Longrightarrow$ (2): 设 S 是亚正锥 T 在 K 上的一个拓展, 则易知, $S_K(T)\subseteq S$. 由于 $-1\notin S$, 从而 $-1\notin S_K(T)$.

(2) $\Longrightarrow$ (3): 由于 $-1\notin S_K(T)$, 从而易知, $S_K(T)$ 是 K 的一个亚正锥. 由定理 1.1.2 的推论知, K 有一个正锥 Q, 使得 $S_K(T)\subseteq Q$. 自然有, $T\subseteq Q$.

(3) $\Longrightarrow$ (1): 注意到, 正锥总为亚正锥. 从而结论显然. 证毕.

由上面定理可知, 若 K 是域 F 的纯超越扩张, 则对于 F 的任意亚正锥 T, K 是 (F,T) 的实扩张. 此外, 再结合定理 1.1.2, 我们可以建立下面结果.

命题 1.3.2 设 (F,T) 是一个亚序域, K 是 F 的一个扩张, 则有

$$S_K(T)=\bigcap_{Q}Q,$$

这里 Q 取遍 K 的所有包含 T 的正锥.

证明 由定理 1.1.2 知,

$$S_K(T)=\bigcap_Q Q,$$

其中 Q 取遍 K 的所有包含 $S_K(T)$ 的正锥. 注意到, 对于 K 的正锥 $Q, T\subseteq Q$ 当且仅当 $S_K(T)\subseteq Q$. 因此, 上面命题获证.

一般说来, 亚序域的代数扩张未必为实扩张, 例如对于任意亚序域 (F,T), $F(\sqrt{-1})$ 不是它的实扩张, 对于单代数扩张, 我们可以给出它为实扩张的一个如下充分条件.

命题 1.3.3 设 (F,T) 是亚序域, α 是 F 上代数元, 且 $f(x)$ 是 α 在 F 上的极小多项式. 若对于某两个元素 $a, b\in F$, $f(a)f(b)\notin T$, 则 $F(\alpha)$ 为 (F,T) 的实扩张.

证明 假若命题不成立, 则由自然数的良序性, 我们可选取 F 上这样的代数元 α, 使得 (i) 对于某两个 $a, b\in F$, $f(a)f(b)\notin T$, 这里 $f(x)$ 是 α 在 F 上的极小多项式; (ii)$F(\alpha)$ 不是 (F,T) 的实扩张; (iii) 在保证条件 (i) 和 (ii) 成立的前提下, α 在 F 上的极小多项式 $f(x)$ 的次数 n 最小. 此时, 由定理 1.3.1 知, $-1\in S_{F(\alpha)}(T)$. 根据单代数扩张中的元素形式知, 存在域 F 上次数不超过 $n-1$ 的多项式 $f_i(x)$, $i=1,\cdots,r$, 使得

$$-1=\sum_{i=1}^r t_if_i(\alpha)^2,$$

即

$$1+\sum_{i=1}^r t_if_i(\alpha)^2=0,$$

其中 $t_i\in T$, $i=1,\cdots,r$.

由此有 $1+\sum\limits_{i=1}^r t_if_i(x)^2=f(x)g(x)$, 对于 $F[x]$ 中某个次数小于 n 的多项式 $g(x)$. 此时有

$$1+\sum_{i=1}^r t_if_i(a)^2=f(a)g(a),\ 1+\sum_{i=1}^r t_if_i(b)^2=f(b)g(b).$$

从而有 $g(a)g(b)\neq 0$, 且 $\big(f(a)f(b)\big)\big(g(a)g(b)\big)\in T$. 由条件 (i) 可知, $g(a)g(b)\notin T$. 因此, $g(x)$ 至少有一个不可约因式 $h(x)$, 使得 $h(a)h(b)\notin T$. 令 β 是 $h(x)$ 在 F 的代数闭包中的一个根. 显然, $h(x)$ 的次数低于 n. 由条件 (iii) 可知, $F(\beta)$ 是 (F,T) 的实扩张. 然而, 我们有 $1+\sum\limits_{i=1}^r t_if_i(\beta)^2=f(\beta)g(\beta)=0$, 即有 $-1\in S_{F(\beta)}(T)$, 矛盾. 从而定理获证.

由命题 1.3.3, 立即有如下定理.

定理 1.3.4 设 $(F, \leqslant)$ 是序域, α 是 F 上代数元, 且 $f(x)$ 是 α 在 F 上的极小多项式. 若对于某两个元素 $a, b \in F$, $f(a)f(b) < 0$, 则 $\leqslant$ 可以拓展为 $F(\alpha)$ 上的一个序.

证明 设 P 是与 $\leqslant$ 相对应的正锥, 则 $f(a)f(b) \notin P$. 由命题 1.3.3 知, $F(\alpha)$ 是 (F, P) 的实扩张. 从而 $F(\alpha)$ 有一个正锥 Q, 使得 $P \subseteq Q$. 令 $\leqslant_Q$ 为与 Q 相对应的序, 则 $\leqslant_Q$ 为 $\leqslant$ 在 $F(\alpha)$ 上的一个拓展. 证毕.

推论 1 设 $(F, \leqslant)$ 是一个序域, K 是 F 的一个奇数次扩张, 则序 $\leqslant$ 在 K 上有一个拓展.

证明 由熟知的本原元定理知, $K = F(\alpha)$. 设 $f(x)$ 是 α 在 F 上的极小多项式, 则 $f(x)$ 的次数等于扩张次数 $[K : F]$, 从而为奇数. 令 $f(x) = x^{2n+1} + a_{2n}x^{2n} + \cdots + a_0$, 其中 $a_0, a_1, \cdots, a_{2n} \in F$, 且令 $M = n + 1 + \frac{1}{2}(a_0^2 + a_1^2 + \cdots + a_{2n}^2)$. 易知, $f(M) > 0$, 但 $f(-M) < 0$. 由定理 1.3.4 知, $\leqslant$ 可以拓展为 K 的一个序. 证毕.

推论 2 设 (F, T) 为亚序域, 则对于任意 $a \in T$, $F(\sqrt{a})$ 为 (F, T) 的一个实扩张, 这里 $\sqrt{a}$ 表示多项式 $x^2 - a$ 在 F 的代数闭包中的一个根.

证明 当 $\sqrt{a} \in F$ 时, 结论显然成立. 当 $\sqrt{a} \notin F$ 时, $\sqrt{a}$ 在 F 上的极小多项式为 $x^2 - a$. 此时, $f(0)f(a+1) = -a(a^2 + a + 1) \notin T$. 根据命题 1.3.3, 推论 2 成立.

根据一个序域在它的真代数扩张上是否能拓展序, 我们可以引进如下概念.

定义 1.3.1 一个序域 (F, P) (或 $(F, \leqslant)$) 称作极大序域, 如果 P (或 $\leqslant$) 不能拓展到 F 的任意一个真代数扩张.

例 $(\mathbb{R}, \leqslant)$ 是一个极大序域, 其中 $\leqslant$ 是实数域 $\mathbb{R}$ 上的通常大小关系.

定义 1.3.2 设 (K, Q) 是序域 (F, P) 的一个序扩张. 如果 K 是 F 的一个代数扩张, 且 (K, Q) 是极大序域, 那么称 (K, Q) 为序域 (F, P) 的一个极大序扩张.

对于序域的极大序扩张的存在性, 我们有如下定理.

定理 1.3.5 任何序域都有极大序扩张.

证明 设 (F, P) 是一个序域, 且令 Ω 为 F 的代数闭包. 作如下集合:

$\Xi = \{(L, P_L) \mid L$ 是 F 和 Ω 的中间域, P_L 是正锥 P 在 L 上的一个拓展 $\}$.

显然, $(F, P) \in \Xi$. 此外, 在 Ξ 上可规定如下二元关系 $\preceq$:

$$(L_1, P_1) \preceq (L_2, P_2), \text{ 当且仅当 } L_1 \subseteq L_2, \text{ 且 } P_1 \subseteq P_2.$$

易知, $\preceq$ 是集 Ξ 的一个偏序.

设 $\{(L_\lambda, P_\lambda) \mid \lambda \in \Lambda\}$ 是偏序集 Ξ 中任意一个链, 其中 Λ 是一个指标集. 令 $L_0 = \bigcup\limits_{\lambda \in \Lambda} L_\lambda$, 且 $P_0 = \bigcup\limits_{\lambda \in \Lambda} P_\lambda$. 显然, L_0 是 F 和 Ω 的中间域. 并且容易验证: P_0

是 L_0 的一个正锥. 从而可知, $(L_0, P_0) \in \Xi$, 且 (L_0, P_0) 是所给链 $\{(L_\lambda, P_\lambda) \mid \lambda \in \Lambda\}$ 的一个上界. 由 Zorn 引理知, Ξ 中有极大元 (K, Q). 根据定义 1.3.2, 这个极大元 (K, Q) 即为 (F, P) 的极大序扩张. 证毕.

在下一章中, 我们将讨论序域的极大序扩张的惟一性.

§1.4 阿基米德序和非阿基米德序

本节是围绕一个序域的区间拓扑及其子域的区间拓扑的关系而展开讨论的. 此外, 我们还考虑序域的子域关于区间拓扑的稠密性.

定义 1.4.1 设 $(K, \leqslant)$ 是一个序域, F 是 K 的一个子域. K 中一个非零元素 α 称作 F 上的无限大元素 (或无限小元素), 若对于 F 中每个正元素 a, 总有 $|\alpha| > a$ (或 $|\alpha| < a$). 如果 K 中没有 F 上的无限大元素, 那么称 $\leqslant$ 是在子域 F 上的阿基米德序 , 或称 $(K, \leqslant)$ 是在子域 F 上的阿基米德序域 . 否则, 称 $\leqslant$ 是在子域 F 上的非阿基米德序 , 或称 $(K, \leqslant)$ 是在子域 F 上的非阿基米德序域 . 特别地, 当 $\leqslant$ 是在有理数子域 $\mathbb{Q}$ 上的阿基米德序时, 我们还称 $\leqslant$ 是一个阿基米德序 , 或称 $(K, \leqslant)$ 是一个阿基米德序域 .

例 1 实数域 $\mathbb{R}$ 的惟一序 $\leqslant$ 是阿基米德序. 对于 $\mathbb{R}$ 的任意子域 F, $\leqslant$ 在 F 上的限制也是 F 的阿基米德序.

例 2 考虑 §1.1 中例 3. 对于序 P_{0+}, 元素 t 在子域 F 上是无限小正元素, t^{-1} 是在 F 上的无限大正元素. 而对于序 $P_{+\infty}$ 来说, t 是在 F 上的无限大正元素, t^{-1} 是在 F 上的无限小正元素. 因此, 序 P_{0+} 和 $P_{+\infty}$ 都是在子域 F 上的非阿基米德序. 特别地, 当 $F = \mathbb{Q}$ 时, P 是 $\mathbb{Q}$ 的惟一正锥. 此时, 所规定的 P_{0+} 和 $P_{+\infty}$ 都是域 $\mathbb{Q}(t)$ 的非阿基米德序.

根据定义 1.4.1 可知, 若 $(K, \leqslant)$ 是在子域 F 上的阿基米德序域, 则对于 F 和 K 的任意一个中间域 E, $(K, \leqslant)$ 是在 E 上的阿基米德序域. 由此可知, 若 $(K, \leqslant)$ 是一个阿基米德序域, 则对于 K 的任意子域 F, $(K, \leqslant)$ 是在 F 上的阿基米德序域.

命题 1.4.1 设 $(K, \leqslant)$ 是一个序域, F 是 K 的一个子域, 则下列叙述等价:

(1) $\leqslant$ 是在 F 上的阿基米德序;

(2) K 中没有在 F 上无限小元素;

(3) F 对于由序 $\leqslant_F$ 所诱导的区间拓扑是 K 对于由 $\leqslant$ 所诱导的区间拓扑的子空间, 这里 $\leqslant_F$ 是序 $\leqslant$ 在 F 上的限制.

证明 (1) $\Longleftrightarrow$ (2): 若 K 中有在 F 上的无限小元素 α, 则易知, α^{-1} 是 F 上无限大元素. 反之, 若 K 中有在 F 上的无限大元素 α, 则易知, α^{-1} 是 F 上无限小元素. 这些事实表明叙述 (1) 和 (2) 的等价性.

(2) $\Longrightarrow$ (3): 设 $]a, b[_F$ 是 F 中关于 $\leqslant_F$ 的任意一个开区间, 则显然 $]a, b[_F=$

$]a,b[_K\cap F$, 其中 $]a,b[_K$ 表示 K 中关于 $\leqslant$ 的具有端点 a,b 的开区间. 因而, 为证明叙述 (3), 只须证明: 对于 K 中任意一个关于 $\leqslant$ 的开区间 $]\alpha,\beta[_K$, $]\alpha,\beta[_K\cap F$ 对于由 $\leqslant_F$ 诱导的区间拓扑是 F 的一个开子集. 事实上, 若 $c\in]\alpha,\beta[_K\cap F$, 则 $c-\alpha$, $\beta-c\in K$, 使得 $c-\alpha>0$, 且 $\beta-c>0$. 由 (2) 知, F 中有正元素 a 和 b, 使得 $a<c-\alpha$, 且 $b<\beta-c$. 令 $\delta=\min\{a,b\}$, 则 $\delta\in F$, 且 $\alpha<c-\delta<c+\delta<\beta$. 此时显见, $c\in]c-\delta,c+\delta[_F\subseteq]\alpha,\beta[_K\cap F$. 这表明: $]\alpha,\beta[_K\cap F$ 是 F 的开子集. 因此, 叙述 (3) 获证.

(3) $\Longrightarrow$ (2): 假若 K 中有一个在 F 上无限小元素 α. 不失一般性, 可设 $0<\alpha$. 由定义 1.4.1 可知, $]-\alpha,\alpha[_K\cap F=\{0\}$, 这不可能是 F (关于由 $\leqslant_F$ 诱导的区间拓扑) 的开子集, 矛盾于所设 (3). 证毕.

定理 1.4.2 设 $(F,\leqslant)$ 是一个序域, 且 $\leqslant$ 在 F 的一个子域 E 上是阿基米德序. 如果 $(K,\leqslant_K)$ 是 $(F,\leqslant)$ 的一个序扩张, 且 K 是 F 的代数扩张, 则 $\leqslant_K$ 也是在 E 上的阿基米德序.

证明 对于任意 $\alpha\in K$, 由引理 1.2.2 知, 有 $M\in S_F$, 使得 $|\alpha|<_K M$. 由于 $\leqslant$ 是在 E 上的阿基米德序, 从而有 E 中正元素 a, 使得 $M=|M|<a$. 此时有 $|\alpha|<_K a$. 这表明 $\leqslant_K$ 是在 E 上的阿基米德序. 证毕.

对于阿基米德序, 我们有如下更进一步的结果.

命题 1.4.3 对于一个序域 $(F,\leqslant)$, 下列叙述是等价的:

(1) $\leqslant$ 是一个阿基米德序;

(2) 有理数子域 $\mathbb{Q}$ 对于由 $\leqslant$ 诱导的区间拓扑在 F 中稠密, 即对于 F 的任意开区间 $]a,b[$, $]a,b[\,\cap\mathbb{Q}\neq\phi$.

证明 (1) $\Longrightarrow$ (2): 对于 F 的任意开区间 $]a,b[$, 总有 $0<(b-a)^{-1}$. 由于 $\leqslant$ 是一个阿基米德序, 从而由定义 1.4.1 知, 有自然数 n, 使得 $(b-a)^{-1}<n$. 从而有 $a<a+\dfrac{1}{n}<b$. 同样, 有自然数 m, 使得 $|na|<m$. 由自然数的良序性, 可设 m 是满足该不等式的最小自然数. 由此有 $m-1\leqslant|na|$. 当 $0\leqslant a$ 时, $m-1\leqslant na<m$, 从而有 $a<\dfrac{m}{n}\leqslant a+\dfrac{1}{n}<b$. 当 $a<0$ 时, $m-1\leqslant -na<m$, 从而有 $a\leqslant\dfrac{1-m}{n}<a+\dfrac{1}{n}<b$. 因此, 总有 $]a,b[\,\cap\mathbb{Q}\neq\phi$.

(2) $\Longrightarrow$ (1): 对于每个 $a\in F$, 由 (2) 知, $]|a|,|a|+1[\,\cap\mathbb{Q}\neq\phi$. 从而有 $q\in\mathbb{Q}$, 使得 $|a|<q$. 这表明 F 中没有在 $\mathbb{Q}$ 上无限大元素, 即 $\leqslant$ 是阿基米德序. 证毕.

应该指出, 对于一个序域 $(K,\leqslant)$, 若 K 的一个子域 F 在 K 中稠密, 则通过命题 1.4.3 中蕴含 "(2) $\Longrightarrow$ (1)" 的证明可知, $\leqslant$ 是在 F 上的阿基米德序. 然而, 这一事实的逆命题未必成立, 见下例.

例 3 设 $(F(t),P_{0+})$ 是在 §1.1 的例 3 中所规定的序域, 则 $F(t)$ 显然是子域 $F(t^2)$ 的一个代数扩张. 由引理 1.2.2 可知, $F(t)$ 的序 P_{0+} 是在 $F(t^2)$ 上的阿基米德序. 然而易知, $]t,2t[\,\cap F(t^2)=\phi$.

命题 1.4.4 设 $(K, \leqslant)$ 是一个序域， F 是 K 的一个真子域，则对于由 $\leqslant$ 诱导的区间拓扑，子集 $K \setminus F$ 在 K 中稠密，即对于任意 $u, v \in K$, 其中 $u < v$, 总有 $w \in K$, 使得 $w \notin F$, 但 $u < w < v$.

证明 若 $u \notin F$ 或 $v \notin F$, 则 $u + \frac{1}{2}(v-u)$ 和 $u + \frac{1}{3}(v-u)$ 不同时属于 F, 但都在区间 $]u, v[$ 内. 此时，命题成立. 下设 $u, v \in F$. 任取 K 中一个正元素 α, 使得 $\alpha \notin F$, 且令 $w = u + \alpha(1+\alpha)^{-1}(v-u)$. 此时易知， $w \notin F$, 而 $u < w < v$. 证毕.

现在，我们来证明这样一个事实：每个阿基米德序域实际上"等同于"实数域 $\mathbb{R}$ 的一个子域. 为此，我们需要下面的定义.

定义 1.4.2 设 $(F_1, \leqslant_1)$ 和 $(F_2, \leqslant_2)$ 均为序域. 域 F_1 到 F_2 的一个单同态 π 被称作保序嵌入，若对于 $a, b \in F_1$, $\pi(a) \leqslant_2 \pi(b)$, 只要 $a \leqslant_1 b$. 如果 π 还是满射，那么称 π 是序域 $(F_1, \leqslant_1)$ 到 $(F_2, \leqslant_2)$ 的一个保序同构.

显然， π 是序域 $(F_1, \leqslant_1)$ 到 $(F_2, \leqslant_2)$ 的一个保序嵌入 (同构), 当且仅当 π 是 F_1 到 F_2 的一个单同态 (同构), 且 $\pi(P_1) \subseteq P_2$ $(\pi(P_1) = P_2)$, 其中 P_1 和 P_2 分别为序 $\leqslant_1$ 和 $\leqslant_2$ 的对应正锥.

定理 1.4.5 一个序域 $(F, \leqslant)$ 为阿基米德序域，当且仅当存在一个 $(F, \leqslant)$ 到实数域 $\mathbb{R}$ 的保序嵌入，这里 $\mathbb{R}$ 的惟一序也记作 $\leqslant$. 此时，所要求的保序嵌入是惟一的.

证明 充分性：设 π 是 $(F, \leqslant)$ 到 $\mathbb{R}$ 的一个保序嵌入. 注意到，有理数域 $\mathbb{Q}$ 可看作 F 和 $\mathbb{R}$ 的共同的素子域. 由此易知，映射 π 在 $\mathbb{Q}$ 上的限制是 $\mathbb{Q}$ 到 $\mathbb{R}$ 的恒等嵌入，即对于每个 $q \in \mathbb{Q}$, $\pi(q) = q$.

设 a 是 F 中任意元素，则 $\pi(a) \in \mathbb{R}$. 由于 $\mathbb{R}$ 的惟一序是阿基米德序，从而有 $q \in \mathbb{Q}$, 使得 $|\pi(a)| < q$, 即 $\pi(-q) < \pi(a) < \pi(q)$. 由 π 的保序性可知， $-q < a < q$, 即 $|a| < q$. 这表明 $(F, \leqslant)$ 是阿基米德序域.

必要性：对于任意 $a \in F$, 可作 $\mathbb{Q}$ 的如下子集：

$$S_a := \{q \in \mathbb{Q} \mid q \leqslant a\}.$$

由所设知， $\leqslant$ 是 F 的阿基米德序. 从而有 $q_1 \in \mathbb{Q}$, 使得 $|a| < q_1$. 此时必有 $-q_1 < a < q_1$, 即 $-q_1 \in S_a$. 因而， S_a 是一个有上界 q_1 的非空子集.

注意到 $S_a \subseteq \mathbb{R}$, 从而 S_a 在 $\mathbb{R}$ 中有上确界 $\sup(S_a)$. 据此，我们可作 F 到 $\mathbb{R}$ 中的一个映射 π, 使得对于每个 $a \in F$, $\pi(a) = \sup(S_a)$.

设 $a, b \in F$ 且 $a < b$. 由命题 1.4.3 知，有 $q_1, q_2 \in \mathbb{Q}$, 使得 $a < q_1 < q_2 < b$. 由此有 $\pi(a) = \sup(S_a) \leqslant q_1 < q_2 \leqslant \sup(S_b) = \pi(b)$. 这表明： π 是一个保序的单射.

对于任意小的正有理数 ϵ, 由上确界的定义知，有 $q \in S_a$, 使得 $q > \pi(a) - \epsilon$, 即 $q + \epsilon > \pi(a)$. 从而 $q + \epsilon \notin S_a$, 即有 $a < q + \epsilon$. 由此有 $-(q+\epsilon) \in S_{-a}$. 这样，我们有 $\pi(-a) \geqslant -(q+\epsilon) \geqslant -\pi(a) - \epsilon$. 由 ϵ 的任意性，有 $\pi(-a) \geqslant -\pi(a)$. 另一方面，

对于任意小的正有理数 ϵ 以及每个 $q \in S_a$, 显然 $q-\epsilon < a$, 即有 $-a < -q+\epsilon$. 从而 $\pi(-a) \leqslant -q+\epsilon$, 即对于每个 $q \in S_a$, $q \leqslant -\pi(-a)+\epsilon$. 由此有 $\pi(a) \leqslant -\pi(-a)+\epsilon$. 再由 ϵ 的任意性, 有 $\pi(a) \leqslant -\pi(-a)$. 因而 $\pi(-a) = -\pi(a)$, 对于每个 $a \in F$. 自然有, $\pi(0)=0$.

设 $a, b \in F$, 则显然有 $S_a+S_b \subseteq S_{a+b}$. 从而有 $\pi(a)+\pi(b) = \sup(S_a)+\sup(S_b) \leqslant \sup(S_{a+b}) = \pi(a+b)$. 据此有, $\pi(a+b)-\pi(a) = \pi(a+b)+\pi(-a) \leqslant \pi((a+b)-a) = \pi(b)$. 因而, $\pi(a+b) = \pi(a)+\pi(b)$. 此外, 当 $0<a$ 且 $0<b$ 时, 由前面的讨论知, $0<\pi(a)$ 且 $0<\pi(b)$. 设 ϵ 是任意一个同时小于 $\pi(a)$ 和 $\pi(b)$ 的正有理数, 则有 $q \in S_a$ 和 $r \in S_b$, 使得 $\pi(a) < q+\epsilon$ 和 $\pi(b) < r+\epsilon$. 从而必有 $a < q+\epsilon$, 且 $b < r+\epsilon$, 即有 $ab < (q+\epsilon)(r+\epsilon)$. 于是 $(q+\epsilon)(r+\epsilon)$ 是 S_{ab} 的一个上界. 由此有, $\pi(ab) \leqslant (q+\epsilon)(r+\epsilon)$. 注意到, $0 < q \leqslant \pi(a)$ 且 $0 < r \leqslant \pi(b)$. 从而有 $\pi(ab) \leqslant [\pi(a)+\epsilon][\pi(b)+\epsilon]$. 由 ϵ 的任意小性知, $\pi(ab) \leqslant \pi(a)\pi(b)$. 另一方面, 由于 $0<q\leqslant a$ 且 $0<r\leqslant b$, 从而 $qr \leqslant ab$, 即 $qr \in S_{ab}$. 由此有 $qr \leqslant \pi(ab)$, 即有 $\pi(ab) \geqslant [\pi(a)-\epsilon][\pi(b)-\epsilon]$. 由 ϵ 的任意小性可知, $\pi(ab) \geqslant \pi(a)\pi(b)$. 因而我们有 $\pi(ab) = \pi(a)\pi(b)$. 在此基础上, 借助于上面等式 $\pi(-a) = -\pi(a)$ $(a \in F)$ 可进一步验证: 对于任意 $a, b \in F$, 均有 $\pi(ab) = \pi(a)\pi(b)$.

综上所述, π 是一个保序嵌入.

假若存在另一个 $(F, \leqslant)$ 到实数域 $\mathbb{R}$ 的保序嵌入 τ, 且 $\tau \neq \pi$, 则对于某个 $a \in F$, $\tau(a) \neq \pi(a)$. 不妨设 $\tau(a) < \pi(a)$. 由 $\mathbb{Q}$ 在 $\mathbb{R}$ 中的稠密性, 有 $q \in \mathbb{Q}$, 使得 $\tau(a) < q < \pi(a)$, 即 $\tau(a) < \tau(q) = \pi(q) < \pi(a)$. 由于 τ 和 π 都是保序嵌入, 从而有 $a<q<a$, 矛盾. 因此, 定理所要求的保序嵌入是惟一的. 定理获证.

§1.5 序 空 间

在本节中, 我们把实域上的所有序作为一个整体来考虑. 通过赋予某个拓扑结构, 任意一个实域的所有序将作为一个拓扑空间而得到研究.

设 F 是一个实域, 且 $\mathcal{X}_F$ 表示 F 的所有序(正锥)组成的集合, 即 $\mathcal{X}_F = \{P \mid P$ 为 F 的一个正锥 $\}$. 根据定理 1.1.3 知, $\mathcal{X}_F \neq \phi$. 对于每个 $a \in \dot{F}$, 可作出 $\mathcal{X}_F$ 的如下子集:

$$H(a) := \{P \in \mathcal{X}_F \mid a \in P\}.$$

显然, $H(-1)=\phi$, 而 $H(1)=\mathcal{X}_F$. 根据拓扑学知识可知, 子集族 $\mathcal{H} := \{H(a) \mid a \in \dot{F}\}$ 可作为子基生成 $\mathcal{X}_F$ 的一个拓扑. 对于这样一个拓扑, 其基本开集具有如下形式:

$$H(a_1, \cdots, a_n) := \bigcap_{i=1}^{n} H(a_i),$$

其中 $a_1, \cdots, a_n$ 是 $\dot{F}$ 中有限个元素.

定义 1.5.1 由上面的子集族 $\mathcal{H}$ 作为子基所生成的 $\mathcal{X}_F$ 的拓扑称作 $\mathcal{X}_F$ 的 Harrison 拓扑 . 此时, 具有 Harrison 拓扑的拓扑空间 $\mathcal{X}_F$ 称作域 F 的序空间.

一般说来, 子集族 $\mathcal{H}$ 对于子集的交和并都不是封闭的. 然而, 对于子集的 "对称差", $\mathcal{H}$ 是封闭的. 对于已知集合 S 的两个子集 A 和 B, A 和 B 的对称差规定如次: $A \triangle B := (A \setminus B) \cup (B \setminus A)$.

命题 1.5.1 设 F 是一个实域, 则有:

(1) 对于 $a \in \dot{F}$, $H(a)$ 对于 Harrison 拓扑是既开又闭的子集. 从而对于 $a_1, \cdots, a_n \in \dot{F}$, 基本开集 $H(a_1, \cdots, a_n)$ 也是闭子集;

(2) 对于 $a, b \in \dot{F}$, $H(a) \triangle H(b) = H(-ab)$;

(3) $\mathcal{H}$ 对于 $\triangle$ 组成一个 (交换) 群.

证明 (1) 结论来自于这样的事实: $\mathcal{X}_F \setminus H(a) = H(-a)$, 且 $H(-a)$ 对于 Harrison 拓扑是开子集.

(2) 事实上, $P \in H(-ab)$ 当且仅当 (i)$a \in P$ 且 $-b \in P$; 或者 (ii)$-a \in P$ 且 $b \in P$, 当且仅当 $P \in H(a) \setminus H(b)$ 或 $P \in H(b) \setminus H(a)$, 即 $P \in H(a) \triangle H(b)$.

(3) 根据叙述 (2), $\mathcal{H}$ 对于 $\triangle$ 是封闭的. 显然, $\triangle$ 满足结合律. 此外, 容易验证, $\phi = H(-1)$ 对于 $\triangle$ 来说是 $\mathcal{H}$ 的单位元, 且对于每个 $a \in \dot{F}$, $H(a) \triangle H(a) = \phi$. 因此, $\mathcal{H}$ 对于运算 $\triangle$ 是一个 (交换) 群. 证毕.

由 §1.1 中的讨论知, $\dot{S}_F$ 是 $\dot{F}$ 的一个乘法子群. 这样, 我们可得到商群 $(\dot{F}/\dot{S}_F, \cdot)$.

定理 1.5.2 群 $(\mathcal{H}, \triangle)$ 同构于商群 $(\dot{F}/\dot{S}_F, \cdot)$, 其中相应的同构映射为

$$\pi: \quad H(a) \mapsto -a\dot{S}_F, \quad a \in \dot{F}.$$

证明 作 $\dot{F}$ 到 $\mathcal{H}$ 的如下映射:

$$\tau: \quad a \mapsto H(-a), \quad a \in \dot{F}.$$

由命题 1.5.1(2) 可知, τ 是乘法群 $\dot{F}$ 到群 $\mathcal{H}$ 的一个满同态.

设 $a \in \ker(\tau)$, 则 $H(-a) = \phi$. 从而 $H(a) = \mathcal{X}_F$, 即对于每个 $P \in \mathcal{X}_F$, $a \in P$. 由定理 1.1.4 知, $a \in \bigcap_{P \in \mathcal{X}_F} P = S_F$, 即有 $a \in \dot{S}_F$. 反过来, 当 $a \in \dot{S}_F$ 时, 显然 $H(-a) = \phi$. 因而, $\ker(\tau) = \dot{S}_F$. 由群同态基本定理, τ 诱导出商群 $\dot{F}/\dot{S}_F$ 到 $\mathcal{H}$ 的一个同构映射 $\bar{\tau}$, 使得 $\bar{\tau}(a\dot{S}_F) = H(-a)$, 对于每个 $a \in \dot{F}$. 因此, 令 π 为 $\bar{\tau}$ 的逆映射, 即得定理.

推论 所设同上, 则对于 $a, b \in \dot{F}$, $H(a) = H(b)$ 当且仅当 $ab^{-1} \in \dot{S}_F$.

现在, 我们来研究序空间 $\mathcal{X}_F$ 的拓扑性质.

定理 1.5.3 设 F 是一个实域, 则对于 Harrison 拓扑, $\mathcal{X}_F$ 是一个 Hausdorff 的和全不连通的紧空间.

证明 对于任意两个 $P_1, P_2 \in \mathcal{X}_F$, 其中 $P_1 \neq P_2$, 总有 $a \in P_1$, 使得 $a \notin P_2$. 此时必有 $a \in \dot{F}$. 因而 $P_1 \in H(a)$, 但 $P_2 \notin H(a)$. 由命题 1.5.1(1) 知, $H(a)$ 对于 Harrison 拓扑是 $\mathcal{X}_F$ 的一个既开又闭的子集. 因此, $\mathcal{X}_F$ 对于 Harrison 拓扑是全不连通的.

为证明 $\mathcal{X}_F$ 是一个 Hausdorff 的紧空间, 我们考察从 $\dot{F}$ 到集合 $\{1,-1\}$ 的所有映射组成的集合 $I = \{1,-1\}^{\dot{F}}$. 注意到, I 可看作离散拓扑空间 $\{1,-1\}$ 的乘积空间. 由于 $\{1,-1\}$ 对于离散拓扑是一个 Hausdorff 的紧空间, 从而根据熟知的 Tychonoff 定理, I 的乘积拓扑也是 Hausdorff 的和紧致的.

对于每个 $P \in \mathcal{X}_F$, 我们可以规定这样一个 $\dot{F}$ 到 $\{1,-1\}$ 的 (符号) 映射 sgn_P, 使得对于 $a \in \dot{F}$, 当 $a \in P$ 时, $\mathrm{sgn}_P(a) = 1$; 否则, $\mathrm{sgn}_P(a) = -1$. 据此, 我们有 $\mathcal{X}_F$ 到 I 的如下映射:

$$\mathrm{sgn}: \quad P \mapsto \mathrm{sgn}_P, \quad P \in \mathcal{X}_F.$$

若 $\mathrm{sgn}_{P_1} = \mathrm{sgn}_{P_2}$, 其中 $P_1, P_2 \in \mathcal{X}_F$, 则对于每个 $a \in P_1$, $\mathrm{sgn}_{P_2}(a) = \mathrm{sgn}_{P_1}(a) = 1$, 即 $a \in P_2$. 从而 $P_1 \subseteq P_2$, 必然 $P_1 = P_2$. 这表明: sgn 是一个单射.

由乘积拓扑的定义知, I 的一个子基由如下子集组成:

$$H_a^k := \{f \in I \mid f(a) = k\},$$

这里 $k = 1$ 或 -1, 而 a 取遍 $\dot{F}$ 中全部元素.

容易验证: $\mathrm{sgn}^{-1}(H_a^k) = H(ka)$. 因此, 序空间 $\mathcal{X}_F$ 同胚于 I 的子空间 $\mathrm{sgn}(\mathcal{X}_F)$.

因而, 只须证明: $\mathrm{sgn}(\mathcal{X}_F)$ 作为 I 的子空间是 Hausdorff 的和紧致的. 为此, 只剩下证明: $\mathrm{sgn}(\mathcal{X}_F)$ 是 I 的一个闭子集.

设 $f \in I$, 但 $f \notin \mathrm{sgn}(\mathcal{X}_F)$. 令 $U_f = \{a \in F \mid a = 0 \text{ 或 } f(a) = 1\}$, 则 U_f 不是 F 的一个正锥. 注意到 $U_f \cup -U_f = F$, 从而根据定义 1.1.2 知, 只有如下三种情况:

(1) $U_f = F$. 此时有 $-1 \in U_f$, 即 $f(-1) = 1$. 从而 $f \in H_{-1}^1$, 但 $H_{-1}^1 \cap \mathrm{sgn}(\mathcal{X}_F) = \phi$, 这里 H_{-1}^1 是 I 的一个开子集.

(2) $U_f + U_f \not\subseteq U_f$. 此时, 有 $a, b \in U_f$, 使得 $a + b \notin U_f$. 显然, $a, b \in \dot{F}$, 且 $f(a) = f(b) = 1$. 当 $a+b=0$ 即 $a = -b$ 时, $f \in H_a^1 \cap H_{-a}^1$, 但 $(H_a^1 \cap H_{-a}^1) \cap \mathrm{sgn}(\mathcal{X}_F) = \phi$; 当 $a + b \neq 0$ 时, $f \in H_a^1 \cap H_b^1 \cap H_{a+b}^{-1}$, 但 $(H_a^1 \cap H_b^1 \cap H_{a+b}^{-1}) \cap \mathrm{sgn}(\mathcal{X}_F) = \phi$.

(3) $U_f \cdot U_f \not\subseteq U_f$. 此时, 有 $a, b \in U_f$, 使得 $ab \notin U_f$. 显然, $a, b \in \dot{F}$, $f(a) = f(b) = 1$, 但 $f(ab) = -1$. 于是, $f \in H_a^1 \cap H_b^1 \cap H_{ab}^{-1}$, 但 $(H_a^1 \cap H_b^1 \cap H_{ab}^{-1}) \cap \mathrm{sgn}(\mathcal{X}_F) = \phi$.

由此可见, 总有 f 的一个开邻域, 它和 $\mathrm{sgn}(\mathcal{X}_F)$ 不相交. 因而, $\mathrm{sgn}(\mathcal{X}_F)$ 是 I 的一个闭子集. 证毕.

推论 设 F 是一个实域, 则对于 Harrison 拓扑, $\mathcal{X}_F$ 的既开又闭的子集恰好具有如下形式:

$$H(a_{11},\cdots,a_{1n_1})\cup\cdots\cup H(a_{r1},\cdots,a_{rn_r}),$$

其中 r 为自然数, $a_{ij_i}\in\dot{F}$, $j_i=1,\cdots,n_i$, $i=1,\cdots,r$.

证明 如上形式的子集显然是 $\mathcal{X}_F$ 的既开又闭的子集. 现设 W 是 $\mathcal{X}_F$ 的一个既开又闭的子集. 由于 W 是开的, 从而由 Harrison 拓扑的结构知, W 可表为: $W=\bigcup_{\lambda\in\Lambda}U_\lambda$, 其中 U_λ 是 $\mathcal{X}_F$ 的形如 $H(a_1,\cdots,a_n)$ $(a_i\in\dot{F})$ 的基本开子集, Λ 是一个指标集. 又由于 W 是闭的, 从而由定理 1.5.3 知, W 是 $\mathcal{X}_F$ 的一个紧子集. 于是, 存在有限个 $\lambda_1,\cdots,\lambda_r\in\Lambda$, 使得 $W=U_{\lambda_1}\cup\cdots\cup U_{\lambda_r}$. 证毕.

现设 T 是域 F 的一个亚序. 由定理 1.1.2 及其推论知, $\mathcal{X}_F(T)\neq\phi$, 这里 $\mathcal{X}_F(T)$ 是域 F 的所有包含 T 的正锥 (序) 组成的集合. 显然, $\mathcal{X}_F(T)\subseteq\mathcal{X}_F$. 因而, $\mathcal{X}_F(T)$ 可看作为序空间 $\mathcal{X}_F$ 的一个子空间. 为方便起见, 我们将称子空间 $\mathcal{X}_F(T)$ 为亚序域 (F,T) 的序空间, 且其 (子空间) 拓扑称作 $\mathcal{X}_F(T)$ 的 Harrison 拓扑. 自然, 如下子集组成 $\mathcal{X}_F(T)$ 的一个子基:

$$H^T(a):=H(a)\cap\mathcal{X}_F(T),$$

其中 a 取遍 $\dot{F}$ 中全体元素.

设 $P\in\mathcal{X}_F$, 但 $P\notin\mathcal{X}_F(T)$, 则 $T\not\subseteq P$. 从而有 $a\in T$, 使得 $a\notin P$. 此时显然有, $P\in H(-a)$, 但 $H(-a)\cap\mathcal{X}_F(T)=\phi$. 这表明: $\mathcal{X}_F(T)$ 是序空间 $\mathcal{X}_F$ 的一个闭子集. 结合定理 1.5.3, 我们立即有如下结论.

定理 1.5.4 对于一个亚序域 (F,T), $\mathcal{X}_F(T)$ 对于 Harrison 拓扑是一个 Hausdorff 的和全不连通的紧空间.

仿照前面的讨论, 若记 $\mathcal{H}^T=\{H^T(a)\mid a\in\dot{F}\}$, 则我们可建立如下定理.

定理 1.5.5 设 (F,T) 是一个亚序域, 则 $(\mathcal{H}^T,\triangle)$ 是一个同构于 $\dot{F}/\dot{T}$ 的群, 其中相应的同构映射为

$$H^T(a)\longmapsto -a\dot{T},\quad a\in\dot{F}.$$

定理 1.5.6 设 K 是实域 F 的一个实扩张, 则对于序空间的 Harrison 拓扑, 从 $\mathcal{X}_K$ 到 $\mathcal{X}_F$ 的限制映射 r: $Q\longmapsto Q\cap F$ 是一个连续的闭映射.

证明 由 Harrison 拓扑的定义, 空间 $\mathcal{X}_F$ 的一个子基由形如 $H_F(a)$ $(a\in\dot{F})$ 的子集组成, 这里 $H_F(a)=\{P\in\mathcal{X}_F\mid a\in P\}$. 显然, 对于每个 $a\in\dot{F}$, $r^{-1}(H_F(a))=\{Q\in\mathcal{X}_K\mid a\in Q\}$. 由空间 $\mathcal{X}_K$ 的拓扑结构知, $\{Q\in\mathcal{X}_K\mid a\in Q\}$ 是 $\mathcal{X}_K$ 的开子集. 从而限制映射 r 是连续映射. 注意到, $\mathcal{X}_K$ 是紧空间, 且 $\mathcal{X}_F$ 是 Hausdorff 空间. 由拓扑学知识, r 是一个连续的闭映射. 证毕.

应该注意, 定理 1.5.6 中的限制映射 r 未必是开映射, 见下例.

例 设 $F=\mathbb{Q}(\alpha)$, 其中 α 是任意一个超越实数, 则 $F\subseteq\mathbb{R}$. 注意到, $\mathbb{R}^2$ 是 $\mathbb{R}$ 的惟一正锥. 从而 $\mathcal{X}_\mathbb{R}=\{\mathbb{R}^2\}$. 设 $H(u_1,\cdots,u_n)$ 是 $\mathcal{X}_F$ 的任意一个包含 $\mathbb{R}^2\cap F$ 的基

本开集. 由 F 中元素的形式知, $u_i = \dfrac{f_i(\alpha)}{g_i(\alpha)}$, 其中 $f_i(x), g_i(x) \in \mathbb{Q}[x]$, 且 $g_i(x) \neq 0$, $i = 1, \cdots, n$. 此时有 $0 < \dfrac{f_i(\alpha)}{g_i(\alpha)}$, $i = 1, \cdots, n$, 这里 $\leqslant$ 是 $\mathbb{R}^2 \cap F$ 的对应序. 根据有理函数的连续性以及有理数在 $\mathbb{R}$ 中的稠密性, 存在 $q \in \mathbb{Q}$, 使得 $0 < \dfrac{f_i(q)}{g_i(q)}$, $i = 1, \cdots, n$. 据此, 构造 F 的这样一个子集 P, 使得 $0 \in P$, 且对于 F 中非零元 $\dfrac{f(\alpha)}{g(\alpha)}$, $f(x), g(x) \in \mathbb{Q}[x]$, 有: $\dfrac{f(\alpha)}{g(\alpha)} \in P$, 当且仅当多项式 $f(x+q)g(x+q)$ 的尾项系数为正数. 易知, P 是 F 的一个正锥, 且 $P \in H(u_1, \cdots, u_n)$. 显然 $P \neq \mathbb{R}^2 \cap F$. 这表明 $\{\mathbb{R}^2 \cap F\}$ 不是 $\mathcal{X}_F$ 的开集. 因此, 限制映射 r 不是一个开映射.

第二章　实闭域与序域的实闭包

在本章中，我们介绍一类重要的实域 —— 实闭域，这类实域可以看作在“实性”前提下的“代数闭”域. 实闭域具有实数域 $\mathbb{R}$ 所具有的许多重要性质，例如适合多项式的中间值定理，Rolle 定理以及 Sturm 定理等等. 因此，实闭域在实域理论乃至实代数几何中有着重大作用. 此外，我们研究与已知序域密切相关的实闭域，即已知序域的实闭包. 在本章中，序域的实闭包的存在性和惟一性被证明. 实闭域和序域的实闭包在概念上的关系犹如域论中代数闭域和域的代数闭包.

§2.1　实　闭　域

在这一节中，我们将给出实闭域的定义，同时建立实闭域的一些重要特性.

定义 2.1.1　一个域 R 称作实闭域，如果 R 是一个实域，但它没有真的实代数扩张 (等价于： R 的每个真代数扩张都不再是实域).

显然，实数域 $\mathbb{R}$ 是实闭域的一个范例.

命题 2.1.1　设 R 是一个实闭域，则

(1) $R^2=\{a^2 \mid a\in R\}$ 是 R 的惟一正锥，从而 R 有惟一序.

(2) R 没有奇数次的真代数扩张.

证明　(1) 设 P 是 R 的任意一个正锥，则显然 $R^2\subseteq P$. 对于 $a\in P$, 由定理 1.3.4 的推论 2 知，$R(\sqrt{a})$ 是序域 (R,P) 的一个实代数扩张，这里 $\sqrt{a}$ 表示多项式 x^2-a 在 R 的代数闭包中的一个根. 此时，$R(\sqrt{a})$ 自然为 R 的实代数扩张. 由于 R 没有真的实代数扩张，从而 $R(\sqrt{a})=R$, 即 $\sqrt{a}\in R$. 因而，$a=(\sqrt{a})^2\in R^2$. 于是，我们有 $P=R^2$.

(2) 设 $\leqslant$ 是 R 的惟一序. 假若 R 有一个奇数次的真代数扩张 K, 则由定理 1.3.4 的推论 1 知，序 $\leqslant$ 在 K 上有一个拓展. 这表明 K 是 R 的真的实代数扩张，矛盾于所设. 证毕.

引理 2.1.2　设 F 是一个实域, 且 $F^2\cup -F^2=F$, 则 $F(\sqrt{-1})$ 没有二次扩张.

证明　由于 F 的特征不等于 2, 从而只须证明： $F(\sqrt{-1})$ 中每个元素都是 $F(\sqrt{-1})$ 的某个元素的平方. 设 $\alpha\in F(\sqrt{-1})$, 则 $\alpha=a+b\sqrt{-1}$, 其中 $a, b\in F$. 如若 $b=0$, 则 $\alpha=a\in F=F^2\cup -F^2$. 于是，对于某个 $c\in F$, $\alpha=c^2$, 或者 $\alpha=-c^2=(c\sqrt{-1})^2$. 下设 $b\neq 0$. 由于 F 是一个实域，且 $F=F^2\cup -F^2$, 从而必有 $F^2+F^2\subseteq F^2$. 此外易知， $F^2=F^4$. 于是有 $c\in F$, 使得 $a^2+b^2=c^4$. 此时可断言 $\frac{1}{2}(c^2-a)\in F^2$. 事实上，如若不然，则 $\frac{1}{2}(c^2-a)\in -F^2$. 由此有 $\frac{1}{2}(-c^2-a)=\frac{1}{2}(c^2-a)-c^2\in -(F^2+F^2)\subseteq -F^2$. 此时可得， $-\frac{b^2}{4}=\frac{1}{2}(c^2-a)\cdot$

$\frac{1}{2}(-c^2-a) \in (-F^2)\cdot(-F^2) \subseteq F^2$, 矛盾. 根据这一断言, 有非零元 $d \in F$, 使得 $\frac{1}{2}(c^2-a) = d^2$. 容易验证 $\alpha = (\frac{b}{2d} + d\sqrt{-1})^2$. 证毕.

现在, 我们可建立下面的重要定理, 它是由 E. Artin 和 O. Schreier 所获得的.

定理 2.1.3 对于一个域 R, 下列叙述是等价的:

(1) R 是实闭域;

(2) R^2 是 R 的 (惟一) 正锥, 且 R 上每个奇次数多项式在 R 中有一个根;

(3) $R(\sqrt{-1})$ 是代数闭域, 且 $R \neq R(\sqrt{-1})$.

证明 (1) $\Longrightarrow$ (2): 结论由命题 2.1.1 即得.

(2) $\Longrightarrow$ (3): 由条件可知, R 是一个实域. 从而 $R \neq R(\sqrt{-1})$, 且 R 的特征为零. 设 K 是 $R(\sqrt{-1})$ 的任意有限扩张, 且 N 是 K 在 R 上的正规闭包, 则 $R(\sqrt{-1}) \subseteq K \subseteq N$, 且 N 是 R 的一个有限 Galois 扩张. 用 G 表示 N 在 R 上的 Galois 群. 由群论中 Sylow 定理, G 有一个 Sylow 2- 子群 H. 令 E 是子群 H 的稳定域, 则由 Galois 基本定理知, $[N:E] = |H|$. 从而 $[E:R] = \frac{[N:R]}{[N:E]} = [G:H]$ 是一个奇数. 由本原元定理知, $E = R(\alpha)$. 令 $f(x)$ 是 α 在 R 上的极小多项式, 则 $f(x)$ 在 R 上不可约, 且 $f(x)$ 的次数为奇数 $[G:H]$. 由所设, $f(x)$ 在 R 中有一个根. 这表明: $[G:H]=1$, 即 $G=H$. 因此, $[N:R] = |G|$ 是 2 的一个方幂. 注意到, N 是 $R(\sqrt{-1})$ 的 Galois 扩张, 且 N 在 $R(\sqrt{-1})$ 上的 Galois 群 G_1 是 G 的子群, 从而 G_1 的阶也是 2 的一个方幂. 假若 $|G_1| > 1$, 则 G_1 有一个子群 H_1, 使得 $[G_1:H_1] = 2$. 令 E_1 是 H_1 的稳定域, 则易知, E_1 是 $R(\sqrt{-1})$ 的二次扩张, 与上面的引理 2.1.2 矛盾. 因而 $|G_1| = 1$, 即 $N = R(\sqrt{-1})$. 此时必有 $K = R(\sqrt{-1})$. 由 K 的任意性知, $R(\sqrt{-1})$ 是一个代数闭域.

(3) $\Longrightarrow$ (1): 首先证明, $R^2 + R^2 \subseteq R^2$. 对于 $a, b \in R$, 由于 $R(\sqrt{-1})$ 是代数闭域, 从而有 $c, d \in R$, 使得 $a + b\sqrt{-1} = (c + d\sqrt{-1})^2$. 由于 $\sqrt{-1} \notin R$, 从而有 $a = c^2 - d^2$, 且 $b = 2cd$. 于是 $a^2 + b^2 = (c^2+d^2)^2 \in R^2$. 因而 $R^2 + R^2 \subseteq R^2$, 进而有 $S_R = R^2$. 再由 $\sqrt{-1} \notin R$ 可得, $-1 \notin R^2 = S_R$. 因此, R 是一个实域. 注意到 $R(\sqrt{-1})$ 是 R 仅有的真代数扩张, 且 $R(\sqrt{-1})$ 不是实域. 因此, 由定义 2.1.1 知, R 是实闭域. 证毕.

推论 设 R 是一个实闭域, $\leqslant$ 是 R 的惟一序, 则

(1) R 上的首一不可约多项式恰为一次多项式以及形如 $(x+b)^2 + c^2$ 的二次多项式, 其中 $b, c \in R$, 且 $c \neq 0$.

(2) 若 $f(x) \in R[x]$, 且对于 $a, b \in R$, 其中 $a < b$, $f(a)f(b) < 0$, 则有 $c \in]a, b[$, 使得 $f(c) = 0$.

证明 (1) 设 $f(x) = (x+b)^2 + c^2$ 是如上所示的二次多项式, 则对于每个 $\alpha \in R$, $f(\alpha) = (\alpha+b)^2 + c^2 > 0$. 这表明: $f(x)$ 在 R 中无根, 从而 $f(x)$ 在 R 上不可约.

反过来，设 $f(x)$ 是 R 上任意一个首一不可约多项式. 由上面定理知，$R(\sqrt{-1})$ 是代数闭域. 从而 $f(x)$ 在 $R(\sqrt{-1})$ 有一个根 $b+c\sqrt{-1}$, 其中 $b,\,c\in R$.

当 $c=0$ 时，$x-b\in R[x]$, 且在 $R[x]$ 中，$(x-b)|f(x)$. 由 $f(x)$ 的不可约性与首一性知，$f(x)=x-b$. 当 $c\neq 0$ 时，令 $p(x)=(x-b-c\sqrt{-1})(x-b+c\sqrt{-1})=(x-b)^2+c^2$, 则 $p(x)\in R[x]$, 且显然 $p(x)$ 在 R 中无根. 因而，二次多项式 $p(x)$ 在 R 上不可约. 注意到，$p(x)$ 与 $f(x)$ 不互素，从而在 $R[x]$ 中，$p(x)|f(x)$. 由 $f(x)$ 的不可约性和首一性知，$f(x)=p(x)$. 从而叙述 (1) 获证.

(2) 由所设知，$f(x)$ 的次数大于零. 将 $f(x)$ 在 $R[x]$ 中分解如下：

$$f(x)=ep_1(x)\cdots p_r(x),$$

其中 e 为 $f(x)$ 的首项系数，且 $p_i(x)$ 是 $R[x]$ 中首一不可约多项式，$i=1,\cdots,r$.

由已知条件知，$e^2[p_1(a)p_1(b)]\cdots[p_r(a)p_r(b)]=f(a)f(b)<0$. 从而对于某个 $j\in\{1,\cdots,r\}$, $p_j(a)p_j(b)<0$. 根据叙述 (1) 可知，$p_j(x)$ 只能是一次多项式，即 $p_j(x)=x-c$, 其中 $c\in R$. 此时必有 $c\in]a,b[$, 且 $f(c)=0$. 证毕.

实闭域的存在是相当普遍的，这可以从下面命题看出.

命题 2.1.4 设 Ω 是一个特征为零的代数闭域，则存在一个实闭域 R, 使得 $\Omega=R(\sqrt{-1})$.

证明 由于 Ω 的特征为零，从而可认定 Ω 包含有理数域 $\mathbb{Q}$. 设 T 是 Ω 在 $\mathbb{Q}$ 上的一个超越基，且令 $F=\mathbb{Q}(T)$. 根据定理 1.3.1 可知，F 是一个实域.

作如下集合

$$\Xi=\{K\mid K \text{ 是 } F \text{ 和 } \Omega \text{ 的中间域，且 } K \text{ 是实域 }\}.$$

注意到 $F\in\Xi$, 从而 $\Xi\neq\phi$. 显然，Ξ 对于集合的包含关系是一个偏序集.

对于 Ξ 中任意一个链 $\{K_\lambda\mid\lambda\in\Lambda\}$, 这里 Λ 为一个指标集，令 $K=\bigcup_{\lambda\in\Lambda}K_\lambda$. 由定义 1.1.1 可验证，$K$ 是一个实域，即 $K\in\Xi$. 因而，链 $\{K_\lambda\mid\lambda\in\Lambda\}$ 在 Ξ 中有上界 K. 由 Zorn 引理可知，Ξ 中有一个极大元 R. 注意到，Ω 是 R 的代数闭包. 从而由 R 的极大性可知，R 是一个实闭域. 根据定理 2.1.3 知，$R(\sqrt{-1})$ 是代数闭域. 此时必有，$\Omega=R(\sqrt{-1})$. 证毕.

此外，根据定理 2.1.3, 我们可以建立下面事实.

命题 2.1.5 设 R 是一个实闭域，F 是 R 的一个子域，则 F 在 R 中的代数闭包也是一个实闭域.

证明 设 F 在 R 中的代数闭包为 A, 则易知，$R^2\cap A$ 是域 A 的一个正锥. 对于 $a\in R^2\cap A$, 则 $a\in A$, 且有 $\alpha\in R$, 使得 $a=\alpha^2$. 显然，α 也是 F 上代数元，即 $\alpha\in A$. 从而 $R^2\cap A\subseteq A^2$. 此时必有 $R^2\cap A=A^2$. 由定理 1.1.4 的推论知，A^2 是域 A 的惟一正锥. 再设 $f(x)\in A[x]$ 是任意一个奇次数多项式. 由定理 2.1.3 知，

$f(x)$ 在 R 中有一个根 β. 显然, β 也是 F 上代数元, 即 $\beta \in A$. 再根据定理 2.1.3, A 是一个实闭域. 证毕.

实闭域具备实数域 $\mathbb{R}$ 所具有的许多重要的代数性质. 下面列出实闭域的一些重要性质. 一个序域 $(F, \leqslant)$ 称作满足中间值定理, 如果对于任意 $f(x) \in F[x]$, 只要 $f(a) < r < f(b)$, 其中 $a, b, r \in F$, 总有 $c \in F$, 使得 $f(c) = r$, 而且 $a < c < b$ 或 $b < c < a$.

定理 2.1.6 设 R 是一个实域, 则 R 是一个实闭域, 当且仅当 R 有一个序 $\leqslant$, 使得 $(R, \leqslant)$ 满足中间值定理.

证明 设 R 是一个实闭域, 且记 $\leqslant$ 是 R 的惟一序. 若 $f(x) \in R[x]$, 使得 $f(a) < r < f(b)$, 其中 $a, b, r \in R$, 则 $[f(a) - r][f(b) - r] < 0$. 显然 $a \neq b$, 不妨设 $a < b$. 由定理 2.1.3 的推论知, 有 $c \in]a, b[$, 使得 $f(c) - r = 0$, 即 $f(c) = r$. 因此, $(R, \leqslant)$ 满足中间值定理.

现设 R 有一个序 $\leqslant$, 使得 $(R, \leqslant)$ 满足中间值定理. 令 P 是序 $\leqslant$ 的对应正锥. 对于任意非零 $a \in P$, 则 $f(x) = x^2 - a \in R[x]$, 使得 $f(0) < 0 < f(a+1)$. 由于 $(R, \leqslant)$ 满足中间值定理, 从而有 $c \in]0, a+1[$, 使得 $f(c) = 0$. 此时有 $a = c^2 \in R^2$, 即有 $P \subseteq R^2$. 从而必有 $P = R^2$. 这表明: R^2 是 R 的惟一正锥. 再设 $f(x) \in R[x]$ 是任意一个奇次数多项式. 根据定理 1.3.4 的推论 1 的证明知, 有 $M \in R$, 使得 $f(-M) < 0 < f(M)$. 由于 $(R, \leqslant)$ 满足中间值定理, 从而有 $b \in R$, 使得 $f(b) = 0$. 由定理 2.1.3 知, R 是一个实闭域. 证毕.

由上面的证明, 我们立即有如下结论.

推论 设 R 是一个实闭域, $\leqslant$ 是 R 的惟一序, 则 $(R, \leqslant)$ 满足中间值定理.

上面推论称作适合实闭域的中间值定理. 此外, 我们还可以证明, 实闭域满足如下关于多项式的 Rolle 定理.

定理 2.1.7 (Rolle 定理) 设 R 是一个实闭域, $\leqslant$ 为 R 的惟一序, $f(x) \in R[x]$. 若对于 $a, b \in R$, 其中 $a < b$, $f(a) = f(b)$, 则有 $c \in]a, b[$, 使得 $f'(c) = 0$, 这里 $f'(x)$ 是多项式 $f(x)$ 的微商 (导数).

证明 令 $g(x) = f(x) - f(a)$, 则 a 和 b 都是 $g(x)$ 在 R 中的根. 由于 $g(x)$ 在 R 中只有有限个根, 从而 $g(x)$ 的所有大于 a 的根 (包括 b) 中必有最小者 d. 此时, 显然 $a < d \leqslant b$, 且 $g(x)$ 在开区间 $]a, d[$ 中没有根. 令 $g(x) = (x-a)^s(x-d)^t h(x)$, 其中 s 和 t 均为自然数, $h(x) \in R[x]$, 且 $h(a)h(d) \neq 0$. 由此有 $f'(x) = g'(x) = s(x-a)^{s-1}(x-d)^t h(x) + t(x-a)^s(x-d)^{t-1}h(x) + (x-a)^s(x-d)^t h'(x) = (x-a)^{s-1}(x-d)^{t-1}u(x)$, 这里 $u(x) = s(x-d)h(x) + t(x-a)h(x) + (x-a)(x-d)h'(x)$. 于是 $u(a)u(d) = -st(a-d)^2 h(a)h(d)$. 假若 $h(a)h(d) < 0$, 则由定理 2.1.3 的推论知, 有 $e \in]a, d[$, 使得 $h(e) = 0$. 此时显然有 $g(e) = 0$, 矛盾于有关 d 的选定. 从而 $h(a)h(d) > 0$, 即有 $u(a)u(d) < 0$. 再由定理 2.1.3 的推论知, 有 $c \in]a, d[$, 使得

$u(c)=0$. 这样， $c\in]a,b[$, 且 $f'(c)=0$. 证毕.

当然，实闭域还有其他重要性质，我们将在后面加以讨论.

§2.2 实闭域的另一刻画

根据上节中定理 2.1.3 可知，若 R 是实闭域，则 R 的代数闭包是它的有限真扩张. 针对这一结论的逆命题， E. Artin 和 O. Schreier 证实了如下论断.

定理 2.2.1 设 R 是一个域， Ω 是 R 的代数闭包，且 Ω 是 R 的一个有限真扩张，则 R 是一个实闭域.

为证明定理 2.2.1, 我们需要建立如下几个涉及到域论的有关引理，这些引理可在有关文献中找到.

引理 2.2.2 设 F 是一个特征为素数 p 的域， $a\in F$ 但 $a\notin F^p$, 则对于任意自然数 e, $x^{p^e}-a$ 在 $F[x]$ 中不可约.

证明 设 Ω 为 F 的代数闭包, 则 $x^{p^e}-a$ 在 Ω 中有一个根 α. 由于 $\alpha^{p^e}=a\in F$, 从而 α 是 F 上的纯不可分元. 因此， α 在 F 上的极小多项式具有这样的形式: $f(x)=x^{p^m}-b$, 其中 m 为非负整数， $b\in F$. 此时显然有， $f(x)|x^{p^e}-a$. 假若 $f(x)\neq x^{p^e}-a$, 则必然 $m<e$. 由此有 $a=\alpha^{p^e}=b^{p^{e-m}}\in F^p$, 矛盾. 因而 $f(x)=x^{p^e}-a$, 即 $x^{p^e}-a$ 在 $F[x]$ 中不可约. 证毕.

引理 2.2.3 设 F 是一个特征为素数 p 的域， $x^p-x-a\in F[x]$, 则 x^p-x-a 在 F 中有根，当且仅当 x^p-x-a 在 $F[x]$ 中可约.

证明 必要性显然. 现设 x^p-x-a 在 $F[x]$ 中可约, 则有 $x^p-x-a=f(x)g(x)$, 其中 $f(x)$, $g(x)$ 是 $F[x]$ 中首一多项式， 且 $1\leqslant\deg f(x)<p$. 令 α 是 x^p-x-a 在 F 的代数闭包中的一个根，则易验证： $\alpha+1,\cdots,\alpha+(p-1)$ 也是 x^p-x-a 的根，由此有

$$x^p-x-a=(x-\alpha)(x-\alpha-1)\cdots(x-\alpha-p+1).$$

令 $k:=\deg f(x)$, 从而有 $f(x)=(x-\alpha-j_1)\cdots(x-\alpha-j_k)$, 这里 $j_1,\cdots,j_k$ 为 $0,1,\cdots,p-1$ 中某 k 个相异元素. 由此可见, $f(x)$ 中项 x^{k-1} 的系数为 $-(k\alpha+j_1+\cdots+j_k)\in F$. 注意到， $j_1+\cdots+j_k\in F$, 从而有 $k\alpha\in F$. 显然， k 与 p 互素. 于是有整数 s 和 t, 使得 $sk+tp=1$. 由此可得， $\alpha=s(k\alpha)+(tp)\alpha=s(k\alpha)\in F$. 这表明： x^p-x-a 在 F 中有根 α. 证毕.

引理 2.2.4 设 F 是一个含有 q 次本原单位根的域，其中 q 为素数， $x^q-a\in F[x]$, 则 x^q-a 在 F 中有根，当且仅当 x^q-a 在 $F[x]$ 中可约.

证明 必要性显然. 现设在 $F[x]$ 中有如下分解式： $x^q-a=f(x)g(x)$, 其中 $f(x)$, $g(x)$ 是 $F[x]$ 中首一多项式，且 $1\leqslant\deg f(x)<q$. 令 α 是 x^q-a 在 F 的代数闭包中的一个根，则易验证： $\alpha\xi,\cdots,\alpha\xi^{q-1}$ 也是 x^q-a 的根，其中 ξ 是 F 中一

个 q 次本原单位根. 由此有

$$x^q - a = (x-\alpha)(x-\alpha\xi)\cdots(x-\alpha\xi^{q-1}).$$

令 $k := \deg f(x)$, 从而有 $f(x) = (x-\alpha\xi^{j_1})\cdots(x-\alpha\xi^{j_k})$, 这里 $j_1, \cdots, j_k$ 为 $0, 1, \cdots, q-1$ 中某 k 个整数. 显然, $f(x)$ 的常项为 $(-1)^k\alpha^k\xi^{j_1+\cdots+j_k} \in F$. 注意到, $\xi^{j_1+\cdots+j_k} \in F$, 从而有 $\alpha^k \in F$. 由于 k 与 q 互素, 从而有整数 s 和 t, 使得 $sk+tq=1$. 此时有 $\alpha = (\alpha^k)^s(\alpha^q)^t = (\alpha^k)^s a^t \in F$. 这表明 $x^q - a$ 在 F 中有根 α. 证毕.

引理 2.2.5 设 $n = p^e$, 其中 p 为奇素数, e 为正整数, 则剩余环 $\mathbb{Z}/(n)$ 中全体可逆元对于乘法组成一个循环群.

证明 设 U_{p^e} 是 $\mathbb{Z}/(p^e)$ 中全体可逆元对于乘法组成的群, 则群 U_{p^e} 的阶为 $p^{e-1}(p-1)$.

当 $e=1$ 时, $\mathbb{Z}/(p)$ 是一个含 p 个元素的域. 由有限域的熟知事实, U_p 是一个含 $p-1$ 个元素的循环群. 设 $a+(p)$ 是 U_p 的一个生成元, 其中 $a \in \mathbb{Z}$. 当 $a^{p-1} \not\equiv 1 \pmod{p^2}$ 时, 令 $b=a$; 否则令 $b=a+p$. 当 $a^{p-1} \equiv 1 \pmod{p^2}$ 即 $b=a+p$ 时, $b^p \equiv a^p \equiv a \not\equiv b \pmod{p^2}$. 从而总有 $b^{p-1} \not\equiv 1 \pmod{p^2}$. 记 r 为 U_{p^2} 中元素 $b+(p^2)$ 的阶, 则上式表明: $r \neq p-1$. 此时, 显然有 $b^r \equiv 1 \pmod{p^2}$. 自然有 $b^r \equiv 1 \pmod{p}$, 即 $a^r \equiv 1 \pmod{p}$. 由于 $a+(p)$ 是 U_p 中阶为 $p-1$ 的元素, 从而必有 $(p-1)|r$. 注意到, $r|p(p-1)$, 但 $r \neq p-1$. 从而 $r = p(p-1)$, 即 $b+(p^2)$ 是 U_{p^2} 的生成元.

假定 $b+(p^e)$ 是群 U_{p^e} 的一个生成元, 其中 $e \geqslant 2$. 下面证明: $b+(p^{e+1})$ 是 $U_{p^{e+1}}$ 的生成元. 设 r 是 $b+(p^{e+1})$ 的阶, 则有 $b^r \equiv 1 \pmod{p^{e+1}}$, 自然有 $b^r \equiv 1 \pmod{p^e}$. 由于 $b+(p^e)$ 的阶为 $p^{e-1}(p-1)$, 从而 $p^{e-1}(p-1)|r$. 假若 $r = p^{e-1}(p-1)$, 则 $c^p \equiv 1 \pmod{p^{e+1}}$, 这里 $c = b^{p^{e-2}(p-1)}$. 由此可知 $c \equiv 1 \pmod{p}$. 从而 c 可写作: $c = 1 + kp^t + mp^{t+1}$, 这里 $0<k<p$, $t>0$ 且 m 是一个非负整数. 则 $c^p = (1+kp^t+mp^{t+1})^p = 1 + \binom{p}{1}(k+mp)p^t + \cdots + (k+mp)^p p^{pt}$. 由于 p 是奇素数, 从而 $pt \geqslant t+2$. 于是 $c^p \equiv 1 + kp^{t+1} \pmod{p^{t+2}}$. 假若 $t<e$ 即 $t+2 \leqslant e+1$, 则由等式 $c^p \equiv 1 \pmod{p^{e+1}}$ 可知, $c^p \equiv 1 \pmod{p^{t+2}}$. 于是有 $1+kp^{t+1} \equiv 1 \pmod{p^{t+2}}$, 此同余式不可能成立. 因而, $t \geqslant e$. 从而又有 $c \equiv 1 \pmod{p^e}$, 即 $b^{p^{e-2}(p-1)} \equiv 1 \pmod{p^e}$, 这矛盾于事实: $b+(p^e)$ 的阶为 $p^{e-1}(p-1)$. 这表明: $r \neq p^{e-1}(p-1)$. 注意到, $r|p^e(p-1)$. 因此, $r = p^e(p-1)$, 即 $b+(p^{e+1})$ 是 $U_{p^{e+1}}$ 的生成元.

根据归纳法原理, 引理获证.

引理 2.2.6 设 F 是一个域, $n=p^e$, 这里 $e>0$, p 为一个奇素数, 则 $F(\xi)$ 是 F 的一个循环扩张, 其中 ξ 是一个 n 次本原单位根.

证明 由于 ξ 是 n 次本原单位根, 从而 p 不为 F 的特征. 注意到 $F(\xi)$ 是多项式 x^n-1 在 F 上的分裂域, 且 x^n-1 在 $F(\xi)$ 中不可能有重根. 因而 $F(\xi)$ 是 F

的一个 Galois 扩张. 令 G 是 $F(\xi)$ 在 F 上的 Galois 群. 对于 $\tau\in G$, $\tau(\xi)$ 显然也是一个 n 次本原单位根. 从而有整数 m, 使得 $\tau(\xi)=\xi^m$, 且 m 与 n 互素. 如若另有整数 m_1, 使得 $\tau(\xi)=\xi^{m_1}$, 则 m_1 与 n 互素, 且 $\xi^{m-m_1}=1$. 由于 ξ 是 n 次本原单位根, 从而 $n|m-m_1$, 即 $m+(n)=m_1+(n)$. 因此, $m+(n)$ 是 $\mathbb{Z}/(n)$ 中由 τ 惟一确定的元素, 从而记作 $\phi(\tau)$. 由于 m 与 n 互素, 从而 $\phi(\tau)\in U_n$, 这里 U_n 表示 $\mathbb{Z}/(n)$ 中所有可逆元组成的乘法群. 据此, 我们有群 G 到 U_n 的一个映射 ϕ, 使得对于每个 $\tau\in G$, $\tau\mapsto\phi(\tau)$.

设 $\phi(\tau)=m+(n)$, $\phi(\pi)=k+(n)$, 其中 $\tau,\pi\in G$, 则 $\tau(\xi)=\xi^m$, $\pi(\xi)=\xi^k$. 从而有 $\tau\cdot\pi(\xi)=\tau(\xi^k)=\xi^{mk}$, 即有 $\phi(\tau\cdot\pi)=(mk)+(n)=[m+(n)][k+(n)]=\phi(\tau)\phi(\pi)$. 因此, ϕ 是一个群同态.

设 $\phi(\tau)=1+(n)$, 则 $\tau(\xi)=\xi$, 即 τ 是 G 中恒等自同构. 这表明: ϕ 是单射. 因而, $G\cong\phi(G)$. 由引理 2.2.5 知, U_n 是一个循环群, 从而其子群 $\phi(G)$ 也是循环的. 因此, G 是一个循环群. 证毕.

现在, 我们可以证明定理 2.2.1 如下:

定理 2.2.1 的证明　记 $K=R(\sqrt{-1})$, 且 $m=[\Omega:K]$. 假若 $\Omega\neq K$, 则 m 是一个大于 1 的整数. 如若 K 不是完备域, 则 K 的特征为素数 p, 且 $K^p\neq K$. 从而有 $a\in K$, 使得 $a\notin K^p$. 由引理 2.2.2 知, $x^{p^m}-a$ 在 K 上不可约. 设 α 是 $x^{p^m}-a$ 在 Ω 中一个根, 则 $[K(\alpha):K]=p^m>m=[\Omega:K]$, 矛盾. 从而 K 是一个完备域, 即 Ω 是 K 的可分扩张. 此时, Ω 显然是 K 的一个 Galois 扩张. 令 G 是 Ω 在 K 上的 Galois 群, 则 $|G|=m$. 令 q 是 m 的一个素因子, 则 G 必有一个阶为 q 的循环子群 H. 令 E 是 H 的稳定域, 则由 Galois 基本定理知, H 是 Ω 在 E 上的 Galois 群, 且 $[\Omega:E]=q$. 假若 q 为 K 的特征, 则根据循环扩张 (在扩张次数为特征的幂的情况下) 的熟知事实 (例如参见文献 [52] 中定理 1.16), E 有一个扩张次数为 q^2 的循环扩张, 这是不可能的. 因此, q 不为 K 的特征. 从而对于每个自然数 n, Ω 中含有 q^n 次本原单位根. 令 ξ_1 是 Ω 中一个 q 次本原单位根. 注意到 ξ_1 是 E 上多项式 $x^{q-1}+x^{q-2}+\cdots+1$ 的一个根, 从而 $[E(\xi_1):E]\leqslant q-1$. 又由于 $[E(\xi_1):E]$ 是 q 的因数, 从而必有 $[E(\xi_1):E]=1$, 即 $\xi_1\in E$. 根据循环扩张 (在扩张次数不被特征整除的情况下) 的一个熟知事实 (例如 [52], §1.13 中命题 1), $\Omega=E(\alpha)$, 其中 α 在 E 上的极小多项式为 x^q-a. 现考察多项式 $x^{q^2}-a$, 且设 β 是它在 Ω 中一个根, 则有 $x^{q^2}-a=(x-\beta)(x-\beta\eta)\cdots(x-\beta\eta^{q^2-1})$, 其中 η 是一个 q^2 次本原单位根. 显然, $\beta\notin E$; 否则 E 上不可约多项式 x^q-a 在 E 中有根 β^q. 从而有 $[E(\beta):E]=q$. 设 $g(x)$ 是 β 在 E 上的极小多项式, 则 $g(x)|x^{q^2}-a$, 即有 $g(x)=(x-\beta\eta^{j_1})\cdots(x-\beta\eta^{j_q})$, 其中 $j_1,\cdots,j_q$ 是 $0,1,\cdots,q^2-1$ 中某 q 个整数. 此时, $g(x)$ 的常项为 $(-1)^q\beta^q\xi_2$, 其中 $\xi_2=\eta^{j_1+\cdots+j_q}$ 是一个 q^2 次单位根. 由上面讨论知, $\beta^q\notin E$, 进而必有 $\xi_2\notin E$. 由于 E 包含所有 q 次单位根, 从而 ξ_2 必是一

个 q^2 次本原单位根. 此时, 显然又有 $\Omega = E(\xi_2)$.

记 F 为 Ω 的素子域, 且 ξ_n 是 Ω 中一个 q^n 次本原单位根, $n = 3, 4, \cdots$. 显然, 有如下由域组成的序列:

$$F(\xi_2) \subseteq F(\xi_3) \subseteq \cdots \subseteq F(\xi_n) \subseteq \cdots.$$

当 Ω 的特征为素数时, F 是一个有限域. 因而, 每个 $F(\xi_n)$ 也是有限域, $n = 2, 3, \cdots$. 由于 $F(\xi_n)$ 包含所有 q^n 次单位根, 从而 $F(\xi_n)$ 至少包含 q^n 个元素. 注意到, 当 n 趋于无穷大时, q^n 也趋于无穷大. 从而在上面序列中, 至少有两个相邻的域不相等. 当 Ω 的特征为 0 时, $F = \mathbb{Q}$. 根据有理数域上分圆域的一个熟知事实, $[F(\xi_2) : F] = q(q-1)$, 而 $[F(\xi_3) : F] = q^2(q-1)$. 从而 $F(\xi_2) \neq F(\xi_3)$. 因此, 总有自然数 r, $r \geqslant 2$, 使得 $F(\xi_r) \neq F(\xi_{r+1})$.

此时, 显然 $\xi_{r+1} \notin E$, 从而 $\Omega = E(\xi_{r+1})$, 且 $[E(\xi_{r+1}) : E] = q$. 令 $h(x)$ 是 ξ_{r+1} 在 E 上的极小多项式, 则显然 $h(x) | x^{q^{r+1}} - 1$. 注意到, $F(\xi_{r+1})$ 为 $x^{q^{r+1}} - 1$ 在 F 上的分裂域, 从而 $h(x) \in F(\xi_{r+1})[x]$. 于是 $h(x) \in D[x]$, 这里 $D := E \cap F(\xi_{r+1})$ 是 F 和 $F(\xi_{r+1})$ 的中间域. 从而即得, $[F(\xi_{r+1}) : D] = q$. 再考虑 F 和 $F(\xi_{r+1})$ 的另一中间域 $F(\xi_r)$. 令 $\xi \in \Omega$ 是多项式 $x^q - \xi_r$ 的一个根, 则 $\xi^q = \xi_r$. 此时易知, ξ 是一个 q^{r+1} 次本原单位根. 从而 $F(\xi_{r+1}) = F(\xi)$. 由 r 的选取知, $\xi \notin F(\xi_r)$. 由引理 2.2.4 知, $x^q - \xi_r$ 在 $F(\xi_r)$ 上不可约. 于是 $[F(\xi_{r+1}) : F(\xi_r)] = [F(\xi) : F(\xi_r)] = q$. 注意到 $\xi_r \notin E$, 从而 $\xi_r \notin D$. 于是 $D \neq F(\xi_r)$. 令 H_1 和 H_2 为 $F(\xi_{r+1})$ 分别在 D 和 $F(\xi_r)$ 上的 Galois 群. 由 Galois 基本定理, H_1 和 H_2 是 G_1 的两个相异的阶为 q 的子群, 这里 G_1 为 $F(\xi_{r+1})$ 在 F 上的 Galois 群. 由于有限循环群的任意两个相同阶的子群必相等, 从而 G_1 不是一个循环群. 由引理 2.2.6 知, $q = 2$. 这表明: $\xi_2 = \pm\sqrt{-1}$, 矛盾于事实 $\sqrt{-1} \in E$. 因此, $\Omega = K = R(\sqrt{-1})$. 由于 Ω 是 R 的真扩张, 从而 $R \neq R(\sqrt{-1})$. 根据定理 2.1.3, R 是一个实闭域. 证毕.

根据定理 2.2.1 及其证明, 且添加适当的文字叙述, 我们不难证明下面的定理 2.2.7. 定理 2.2.7 的详细证明留待读者完成.

定理 2.2.7 设 R 是一个域, Ω 是 R 的代数闭包, 则下列叙述等价:

(1) R 是一个实闭域;

(2) Ω 是 R 的有限扩张, 且 $\Omega \neq R$;

(3) $\Omega \neq R$, 且存在一个自然数 N, 使得 R 上每个不可约多项式的次数都不超过 N.

§2.3 序域的实闭包

在这一节, 我们研究与已知序域密切相关的一类实闭域, 这类实闭域和已知序域的紧密关系可从下面定义中看出.

定义 2.3.1 设 $(F, \leqslant)$ 是一个序域. 一个实闭域 R 称作序域 $(F, \leqslant)$ 的一个实闭包，如果 R 是 F 的代数扩张，且 R 的惟一序是 $\leqslant$ 在 R 上的拓展. 此时，亦称 R 是序域 (F, P) 的一个实闭包，这里 P 是序 $\leqslant$ 的对应正锥.

由上面定义以及序和正锥之间的相互转化易见，一个实闭域 R 是序域 (F, P) 的实闭包，当且仅当 R 是 F 的代数扩张，且 $P \subseteq R^2$. 此外，若 R 是序域 (F, P)（或 $(F, \leqslant)$）的一个实闭包，则由定理 2.1.3 知，$R(\sqrt{-1})$ 是 F 的代数闭包.

首先面临的问题是考虑序域的实闭包的存在性.

定理 2.3.1 任意序域 (F, P) 都有一个实闭包.

证明 由定理 1.3.5 知，序域 (F, P) 有一个极大序扩张 (R, Q). 下面证明 R 是一个实闭域.

对于 $a \in Q$, 由定理 1.3.4 的推论 2 知，$R(\sqrt{a})$ 有一个正锥 Q_a, 使得 $Q_a \cap R = Q$. 由于 (R, Q) 是极大序域且 $R(\sqrt{a})$ 是 R 的代数扩张，从而必有 $R(\sqrt{a}) = R$, 即 $\sqrt{a} \in R$. 于是对于每个 $a \in Q$, $a = (\sqrt{a})^2 \in R^2$, 即有 $Q \subseteq R^2$. 由此有，$Q = R^2$. 由定理 1.1.4 的推论知，R^2 是 R 的惟一正锥.

再设 $f(x)$ 是任意一个奇次数多项式，则 $f(x)$ 至少有一个奇次数的不可约因式 $p(x)$. 设 α 是 $p(x)$ 在 R 的代数闭包中的一个根，则 $R(\alpha)$ 是 R 的一个奇次数扩张. 由定理 1.3.4 的推论 1 知，(R, Q) 有一个序扩张 $(R(\alpha), Q_1)$. 由于 (R, Q) 是极大序域，从而又有 $R(\alpha) = R$, 即 $\alpha \in R$. 因此，$f(x)$ 在 R 中有一个根 α.

根据定理 2.1.3 知，R 是一个实闭域. 注意到 $P \subseteq Q = R^2$. 从而由定义 2.3.1 可知，R 是序域 (F, P) 的实闭包. 证毕.

由上面的证明可见，一个序域的“极大序扩张”和“实闭包”是两个相近的概念，它们的元素组成同一个实闭域，而是否特别标明惟一序是它们之间的仅有差异. 为明确起见，我们给出下面命题.

命题 2.3.2 设 (F, P) 是一个序域，R 是域 F 的一个扩张，则下列叙述等价:

(1) R 是 (F, P) 的一个实闭包;

(2) (R, R^2) 是 (F, P) 的一个极大序扩张.

证明 “(2) $\Longrightarrow$ (1)” 可参考定理 2.3.1 的证明. 现设 R 是 (F, P) 的一个实闭包，则由定理 2.1.3 知，R 仅有真代数扩张 $R(\sqrt{-1})$. 由于 $R(\sqrt{-1})$ 不是实域，自然 R^2 不能拓展为 $R(\sqrt{-1})$ 的一个正锥. 这表明 (R, R^2) 是 (F, P) 的一个极大序扩张. 证毕.

推论 设 (F, P) 是一个序域，则 (F, P) 是一个极大序域，当且仅当 F 是一个实闭域，且 $P = F^2$.

为证明 (序域的) 实闭包的惟一性，我们需要一个方法，用来判定序域上一个多项式在实闭包中究竟有多少个根. 下面给出一个与二次型理论有关的判别方法，这就是著名的 Sylvester 定理.

设 (F,P) 是一个序域，$f(x)\in F[x]$ 是一个 n 次多项式，$n>0$. 令 R 是 (F,P) 的一个实闭包，则由定理 2.1.3 知，$R(\sqrt{-1})$ 是 F 的代数闭包. 从而 $f(x)$ 在 $R(\sqrt{-1})[x]$ 中可分解为 $f(x)=a(x-\alpha_1)\cdots(x-\alpha_n)$, 其中 $a\in F$, $\alpha_i\in R(\sqrt{-1})$, $i=1,\cdots,n$.

对于每个非负整数 k, 记 $\sigma_k:=\sum\limits_{i=1}^{n}\alpha_i^k$. 根据对称多项式的基本事实，每个 σ_k 都可表为含 $f(x)$ 的系数的一个整系数多项式. 从而 $\sigma_k\in F$. 据此，我们可以得到 F 上的如下二次型:

$$\rho_f:=\sum_{i=1}^{n}\sum_{j=1}^{n}\sigma_{i+j-2x_ix_j}.$$

由二次型理论知，我们有一个切实可行的(构造性)方法，可寻求到一个系数在 F 中的非退化线性替换，使得二次型 ρ_f 可化为仅含平方项的标准型: $\sum\limits_{i=1}^{n}a_iy_i^2$, 其中 $a_i\in F$, $i=1,\cdots,n$.

由二次型理论中的熟知事实知，序列 $(a_1,\cdots,a_n)$ 中正元素个数和负元素个数总是保持不变的, 无论所寻求的非退化线性替换是何种形式. 因此, 序列 $(a_1,\cdots,a_n)$ 中正元素个数与负元素个数之差由二次型 ρ_f 惟一确定；这个差称做二次型 ρ_f 的符号差，且记作 $\mathrm{sgn}_P(\rho_f)$.

应该注意到这样的一个事实: 若 (K,Q) 是序域 (F,P) 的一个序扩张, 则 ρ_f 也可看做 K 上一个二次型, 且 $\mathrm{sgn}_Q(\rho_f)=\mathrm{sgn}_P(\rho_f)$. 因而, 我们有 $\mathrm{sgn}_P(\rho_f)=\mathrm{sgn}_{R^2}(\rho_f)$, 只要 R 是序域 (F,P) 的一个实闭包. 据此，我们无需先将二次型 ρ_f 的系数表示为 F 中元素，而仅需通过域 R 上非退化线性替换将二次型 ρ_f 化成标准型，以确定 $\mathrm{sgn}_P(\rho_f)$.

下面的定理是由 J. J. Sylvester 建立的. 这一定理表明: 序域上一个多项式 f 在实闭包中的相异根的个数，仅与二次型 ρ_f 的符号差有关，而与所选取的实闭包的形式无关.

定理 2.3.3 设 (F,P) 是一个序域，$f(x)$ 是 F 上一个 n 次多项式, 其中 $n>0$, 则对于 (F,P) 的任一实闭包 R, $f(x)$ 在 R 中相异根的个数等于 $\mathrm{sgn}_P(\rho_f)$, 这里 ρ_f 是如上规定的 F 上二次型.

证明 设 $f(x)$ 在 R 中的全部相异根为 $\alpha_1,\cdots,\alpha_r$, 且它们的重数分别为 $m_1,\cdots,m_r$.

由定理 2.1.3 的推论可知，多项式 $f(x)$ 在 $R(\sqrt{-1})$ 中但不在 R 内的根是以 R 上共轭元素的形式成对地出现的. 从而，可设 $f(x)$ 在 $R(\sqrt{-1})$ 中但不在 R 内的其他根为: $\beta_1=a_1+b_1\sqrt{-1}$, $\bar{\beta}_1=a_1-b_1\sqrt{-1}$; $\cdots$; $\beta_t=a_t+b_t\sqrt{-1}$, $\bar{\beta}_t=a_t-b_t\sqrt{-1}$, 其中 $a_v,b_v\in R$, 且 $b_v\neq 0$, $v=1,\cdots,t$. 令 M_v 为根 β_v 和 $\bar{\beta}_v$ 的相同重数，$v=1,\cdots,t$.

由二次型 ρ_f 的规定，我们有

$$\begin{aligned}\rho_f &= \sum_{i=1}^{n}\sum_{j=1}^{n}\left[\sum_{u=1}^{r} m_u\alpha_u^{i+j-2}+\sum_{v=1}^{t}M_v(\beta_v^{i+j-2}+\bar{\beta}_v^{i+j-2})\right]x_ix_j\\ &= \sum_{u=1}^{r} m_u\left(\sum_{i=1}^{n}\alpha_u^{i-1}x_i\right)^2+\sum_{v=1}^{t}M_v\left[\left(\sum_{i=1}^{n}\beta_v^{i-1}x_i\right)^2+\left(\sum_{i=1}^{n}\bar{\beta}_v^{i-1}x_i\right)^2\right].\end{aligned}$$

引进新的变量 $y_1,\cdots,y_{r+2t}$, 使得下面的关系式成立：

$$y_u=\sum_{i=1}^{n}\alpha_u^{i-1}x_i,\ u=1,\cdots,r;$$

$$y_{r+2v-1}=\sum_{i=1}^{n}\frac{1}{2}(\beta_v^{i-1}+\bar{\beta}_v^{i-1})x_i,\ v=1,\cdots,t;$$

$$y_{r+2v}=\sum_{i=1}^{n}\frac{\sqrt{-1}}{2}(\bar{\beta}_v^{i-1}-\beta_v^{i-1})x_i,\ v=1,\cdots,t.$$

在上面关系式中，右端的全部系数显然都属于 R. 不难看出，这些系数组成域 R 上一个 $(r+2t)\times n$ 矩阵，且这个系数矩阵可以通过如下域 $R(\sqrt{-1})$ 上的矩阵 A 进行初等行变换可获得：

$$A=\begin{pmatrix}1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1}\\ \vdots & \vdots & \vdots & & \vdots\\ 1 & \alpha_r & \alpha_r^2 & \cdots & \alpha_r^{n-1}\\ 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{n-1}\\ 1 & \bar{\beta}_1 & \bar{\beta}_1^2 & \cdots & \bar{\beta}_1^{n-1}\\ \vdots & \vdots & \vdots & & \vdots\\ 1 & \beta_t & \beta_t^2 & \cdots & \beta_t^{n-1}\\ 1 & \bar{\beta}_t & \bar{\beta}_t^2 & \cdots & \bar{\beta}_t^{n-1}\end{pmatrix}.$$

由于矩阵 A 的左端 $(r+2t)$ 级子式是一个值不为零的 Vandermonde 行列式，从而 A 的秩为 $r+2t$. 因而，上面关系式右端的系数矩阵的秩也为 $r+2t$, 即它的行向量组是线性无关的. 因此，存在 R 上 $n-(r+2t)$ 个 n 维行向量 $(a_{i1},\cdots,a_{in})$, $i=r+2t+1,\cdots,n$, 使得系数矩阵的全部行向量和这些向量组成秩为 n 的一个线性无关的向量组. 据此，再进一步令

$$y_i=\sum_{j=1}^{n}a_{ij}x_j,\ i=r+2t+1,\cdots,n.$$

于是，这些关系式连同上面的关系式给出了 R 上一个非退化线性替换．通过这个线性替换，ρ_f 化成如下标准型：

$$\rho_f=\sum_{u=1}^{r}m_u y_u^2+\sum_{v=1}^{t}M_v(y_{r+2v-1}^2-y_{r+2v}^2).$$

由此可见，$\mathrm{sgn}_{R^2}(\rho_f)=r$．由上面提及的事实，即有 $\mathrm{sgn}_P(\rho_f)=r$．证毕．

现在，我们着手证明实闭包的惟一性．为此，首先证明如下引理．

引理 2.3.4　设 R_1 和 R_2 都是实闭域，则对于它们的惟一序，R_1 到 R_2 的每个单同态都是保序嵌入．

证明　设 τ 是 R_1 到 R_2 的任意单同态，则对于每个 $a\in R_1, \tau(a^2)=\tau(a)^2\in R_2^2$．这表明：$\tau(R_1^2)\subseteq R_2^2$，即 τ 对于 R_1 和 R_2 的惟一序是保序嵌入．证毕．

引理 2.3.5　设 τ 是序域 (F_1,P_1) 到序域 (F_2,P_2) 的一个保序嵌入，R_1 和 R_2 分别是序域 (F_1,P_1) 和 (F_2,P_2) 的实闭包．若 K 是 F_1 和 R_1 的中间域，且 K 是 F_1 的一个有限扩张，则 τ 可以拓展为序域 $(K,R_1^2\cap K)$ 到 (R_2,R_2^2) 的一个保序嵌入．

证明　由本原元定理，可设 $K=F_1(\alpha)$．记 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$ 是 α 在 F_1 上的极小多项式．由定理 2.3.3 知，$\mathrm{sgn}_{P_1}(\rho_f)>0$．令 $f^\tau(x):=x^n+\tau(a_1)x^{n-1}+\cdots+\tau(a_n)\in F_2[x]$．由于 τ 是一个保序嵌入，从而易知，$\mathrm{sgn}_{P_2}(\rho_{f^\tau})=\mathrm{sgn}_{P_1}(\rho_f)>0$．由定理 2.3.3 知，$f^\tau(x)$ 在 R_2 中有根．由域论的一个熟知事实，τ 可以拓展为 K 到 R_2 中一个嵌入．设 $\pi_1,\cdots,\pi_r$ 是由 τ 所拓展的 K 到 R_2 中全部嵌入．假若 $\pi_1,\cdots,\pi_r$ 都不是所求的保序嵌入，则对于 $i=1,\cdots,r$，有某个 $b_i\in R_1^2\cap K$，使得 $\pi_i(b_i)\notin R_2^2$．此时显然有 $\beta_i\in R_1$，使得 $b_i=\beta_i^2, i=1,\cdots,r$．令 $L=K(\beta_1,\cdots,\beta_r)$，则 L 是 F_1 的一个有限扩张．由上面讨论知，必存在 L 到 R_2 的一个嵌入 π．显然，$\pi|_K$ 是 K 到 R_2 的一个嵌入．从而对于某个 $j\in\{1,\cdots,r\}, \pi|_K=\pi_j$．然而 $\pi_j(b_j)=\pi(b_j)=\pi(\beta_j^2)=\pi(\beta_j)^2\in R_2^2$，矛盾．因此，在 $\pi_1,\cdots,\pi_r$ 中必有一者为所求的保序嵌入．证毕．

借助于 Zorn 引理，上面结论可进一步改善为如下定理．

定理 2.3.6　设 τ 是序域 (F_1,P_1) 到序域 (F_2,P_2) 的一个保序嵌入，R_1 和 R_2 分别是序域 (F_1,P_1) 和 (F_2,P_2) 的实闭包，则 τ 可以拓展为序域 (R_1,R_1^2) 到 (R_2,R_2^2) 的一个 (保序) 嵌入．

证明　考虑如下集合：

$\Xi:=\{(K,\pi)\mid K$ 是 F_1 和 R_1 的中间域，π 是 $(K,R_1^2\cap K)$ 到 (R_2,R_2^2) 的保序嵌入，使得 $\pi|_{F_1}=\tau\}$．

显然，$(F_1,\tau)\in\Xi$．在非空集 Ξ 上按如下方式规定一个二元关系 $\preceq$：

$$(K_1,\pi_1)\preceq(K_2,\pi_2)，当且仅当\ K_1\subseteq K_2，且\ \pi_2|_{K_1}=\pi_1.$$

易知，$\preceq$ 是 Ξ 上一个偏序.

对于 Ξ 中任意一个链 $\{(K_\lambda, \pi_\lambda) \mid \lambda \in \Lambda\}$, 令 $K = \bigcup_{\lambda\in\Lambda} K_\lambda$. 易知，$K$ 是 F_1 和 R_1 的一个中间域. 对于每个 $a \in K$, 必有某个 $\lambda_0 \in \Lambda$, 使得 $a \in K_{\lambda_0}$. 此时有 $\pi_{\lambda_0}(a) \in R_2$. 容易证明：元素 $\pi_{\lambda_0}(a)$ 是由 a 惟一确定的，而与 λ_0 的选取无关. 据此，有一个 K 到 R_2 的映射 π, 使得对于每个 $a \in K$, $\pi(a) = \pi_{\lambda_0}(a)$, 其中 $\pi_{\lambda_0}(a)$ 的意义同上. 进一步可验证：$(K, \pi) \in \Xi$. 因而，链 $\{(K_\lambda, \pi_\lambda) \mid \lambda \in \Lambda\}$ 在 Ξ 中有一个上界 (K, π).

由 Zorn 引理知，Ξ 中有极大元 (L, ϕ). 假若 $L \neq R_1$, 则有 $\alpha \in R_1$, 使得 $\alpha \notin L$. 注意到，ϕ 是序域 $(L, R_1^2 \cap L)$ 到 (R_2, R_2^2) 的一个保序嵌入，且 R_1 和 R_2 分别是序域 $(L, R_1^2 \cap L)$ 和 (R_2, R_2^2) 的实闭包. 由引理 2.3.5 知，ϕ 可以拓展为序域 $(L(\alpha), R_1^2 \cap L(\alpha))$ 到 (R_2, R_2^2) 的一个保序嵌入 ψ. 此时有，$(L(\alpha), \psi) \in \Xi$, 且 $(L, \phi) \prec (L(\alpha), \psi)$, 矛盾于 (L, ϕ) 的极大性. 从而 $L = R_1$, 即 ϕ 是 R_1 到 R_2 的一个嵌入. 证毕.

由定理 2.3.6, 我们立即可建立如下关于实闭包的惟一性的结论.

定理 2.3.7 设 (F, P) 是一个序域，则在 F- 同构的意义下，(F, P) 的实闭包是惟一的.

证明 设 R_1 和 R_2 都是序域 (F, P) 的实闭包，则我们只需证明：存在 R_1 到 R_2 的一个 F- 同构. 设 τ 是 F 上的恒等自同构，则由定理 2.3.6 知，τ 可以拓展为 R_1 到 R_2 的一个嵌入 ϕ.

设 $\beta \in R_2$, 且令 $f(x)$ 是 β 在 F 上的极小多项式. 根据定理 2.1.3 的推论，$f(x)$ 在 $R_1[x]$ 中可分解如下：

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_r)[(x + b_1)^2 + c_1^2] \cdots [(x + b_s)^2 + c_s^2],$$

其中 $\alpha_i, b_j, c_j \in R_1$, 且 $c_j \neq 0$, $i = 1, \cdots, r$; $j = 1, \cdots, s$.

注意到，ϕ 可拓展为多项环 $R_1[x]$ 到 $R_2[x]$ 的一个环同态 Φ, 使得

$$a_0x^n + a_1x^{n-1} + \cdots + a_n \longmapsto \phi(a_0)x^n + \phi(a_{n-1})x^{n-1} + \cdots + \phi(a_n).$$

从而有

$$\begin{aligned} f(x) = \Phi(f(x)) = \ & (x - \phi(\alpha_1)) \cdots (x - \phi(\alpha_r)) \\ & [(x + \phi(b_1))^2 + \phi(c_1)^2] \cdots [(x + \phi(b_s))^2 + \phi(c_s)^2], \end{aligned}$$

其中 $\phi(\alpha_i)$, $\phi(b_j)$, $\phi(c_j) \in R_2$, 且 $\phi(c_j) \neq 0$, $i = 1, \cdots, r$; $j = 1, \cdots, s$. 由 $f(\beta) = 0$ 知，$\beta = \phi(\alpha_k)$, 对于某个 $k \in \{1, \cdots, r\}$. 因此，ϕ 是一个满射，即 ϕ 是 R_1 到 R_2 的一个 F- 同构. 证毕.

鉴于上面定理，当 R 是序域 (F, P) 的一个实闭包时，我们可以确定地称 R 是

序域 (F,P) 的实闭包. 如果 P 是亚序域 (F,T) 一个正锥, 那么称序域 (F,P) 的实闭包为亚序域 (F,T) 的一个实闭包. 特别地, 对于实域 F 的任意一个正锥 P, 序域 (F,P) 的实闭包迳称作 F 的一个实闭包.

推论 设 R 是序域 (F,P) 的实闭包, K_1 和 K_2 都是 F 和 R 的中间域, τ 是 K_1 到 K_2 的一个 F- 同构, 则 τ 是序域 $(K_1, R^2 \cap K_1)$ 到 $(K_2, R^2 \cap K_2)$ 的一个保序同构, 当且仅当 $K_1 = K_2$, 且 τ 是恒等自同构. 特别地, R 上的 F- 自同构必为恒等自同构.

证明 充分性显然, 下证必要性. 设 τ 是所给的保序同构. 注意到, R 既是 $(K_1, R^2 \cap K_1)$ 又是 $(K_2, R^2 \cap K_2)$ 的实闭包. 由定理 2.3.6 知, τ 可以拓展为域 R 上的自同构 π. 为证明必要性, 只剩下证明 π 是 R 上的恒等自同构. 事实上, 如若不然, 则有 $\alpha \in R$, 使得 $\pi(\alpha) \neq \alpha$. 不失一般性, 不妨设 $\alpha < \pi(\alpha)$, 这里 $\leqslant$ 为 R 的惟一序. 由引理 2.3.4 知, ϕ 是一个保序同构. 从而又有 $\pi(\alpha) < \pi^2(\alpha)$. 如此继续下去, 我们可以得到如次无限个 R 中元素: $\alpha < \pi(\alpha) < \cdots < \pi^n(\alpha) < \cdots$. 令 $f(x)$ 是 α 在 F 上的极小多项式. 由于 π 是一个 F- 自同构, 从而 $f(\pi^n(\alpha)) = 0$, $n = 0, 1, 2, \cdots$; 这矛盾于事实: $f(x)$ 在 R 中仅有有限个根. 证毕.

作为上面定理的一个应用, 我们来确定序 (正锥) 在单代数扩张上的拓展个数.

定理 2.3.8 设 (F,P) 是一个序域, R 是它的实闭包, $F(\alpha)$ 是 F 的一个单代数扩张, 且 $f(x)$ 是 α 在 F 上的极小多项式, 则如下三个非负整数相等:

(1) $f(x)$ 在 R 中的根的个数;

(2) $F(\alpha)$ 到 R 中的 F- 嵌入的个数;

(3) 正锥 P 在 $F(\alpha)$ 上的拓展个数.

证明 设 m, n 和 k 分别为如 (1), (2) 和 (3) 所示的非负整数. 由域论中熟知事实知, $m = n$. 设 $F(\alpha)$ 到 R 中的全部 F- 嵌入为 $\pi_1, \cdots, \pi_n$. 令 $Q_i = \pi_i^{-1}(R^2) := \{u \in F(\alpha) \mid \pi_i(u) \in R^2\}$, $i = 1, \cdots, n$. 根据定义可验证, Q_i 是 $F(\alpha)$ 的一个正锥, 且 $P \subseteq Q_i$, $i = 1, \cdots, n$. 若 $Q_i = Q_j$, 其中 $i, j = 1, \cdots, n$, 则可以验证: $\pi_i \circ \pi_j^{-1}$ 是序域 $(\pi_j(F(\alpha)), R^2 \cap \pi_j(F(\alpha)))$ 到 $(\pi_i(F(\alpha)), R^2 \cap \pi_i(F(\alpha)))$ 的一个保序同构, 这里 π_j^{-1} 表示 $F(\alpha)$ 到 $\pi_j(F(\alpha))$ 的同构 π_j 的逆映射. 显然, $\pi_i(F(\alpha))$ 和 $\pi_j(F(\alpha))$ 都是 F 和 R 的中间域, 且 $\pi_i \circ \pi_j^{-1}$ 是一个 F- 同构. 由定理 2.3.7 的推论知, $\pi_i \circ \pi_j^{-1}$ 是恒等自同构, 即有 $\pi_i = \pi_j$. 于是必有 $i = j$. 这表明: 正锥 $Q_1, \cdots, Q_n$ 两两不相等. 因而 $n \leqslant k$.

现设 Q 是正锥 P 在 $F(\alpha)$ 上的任意一个拓展, 且令 R_1 是序域 $(F(\alpha), Q)$ 的实闭包. 显然, R_1 也是序域 (F,P) 的实闭包. 由实闭包的惟一性, 存在 R_1 到 R 的一个 F- 同构 ϕ. 由于 $\phi |_{F(\alpha)}$ 是 $F(\alpha)$ 到 R 中一个 F- 嵌入, 从而对于某个 $s \in \{1, \cdots, n\}$, $\phi |_{F(\alpha)} = \pi_s$. 由引理 2.3.4 知, ϕ 是保序同构, 从而 π_s 是序域

$(F(\alpha), Q)$ 到 (R, R^2) 的保序嵌入. 由此易知, $Q = \pi_s^{-1}(R^2) = Q_s$. 因而, $k \leqslant n$. 这样, 我们有 $n = k$.

根据定理 2.3.3, 上面定理中所指的三个非负整数都等于 $\text{sgn}_P(\rho_f)$, 这里 ρ_f 是由多项式 $f(x)$ 所确定的 F 上二次型.

推论 1 设 (F, P) 是一个序域, $F(\alpha)$ 是 F 的一个单代数扩张, 且 $f(x)$ 是 α 在 F 上的极小多项式, 则正锥 P 在 $F(\alpha)$ 上有拓展, 当且仅当 $\text{sgn}_P(\rho_f) > 0$.

推论 2 设 (F, P) 是一个序域, $a \in P$ 但 $a \notin F^2$, 且 α 是多项式 $x^2 - a$ 在 F 的代数闭包中的一个根, 则正锥 P 在 $F(\alpha)$ 上恰好有两个不同的拓展 Q_1 和 Q_2, 使得 $\alpha \in Q_1$, 但 $-\alpha \in Q_2$.

证明 记 R 是序域 (F, P) 的实闭包. 由所设知, $x^2 - a$ 是 α 在 F 上的极小多项式. 显然 $(1+a)^2 - a >_{R^2} 0$, 但 $0^2 - a <_{R^2} 0$. 由中间值定理知, 在 R 的开区间 $]0, 1+a[$ 中有一个根 $\sqrt{a}$. 显然, $-\sqrt{a}$ 是 $x^2 - a$ 在 R 中的另一个根. 因而, 恰好有两个从 F 到 R 中的 F- 嵌入 π_1 和 π_2, 使得 $\pi_1(\alpha) = \sqrt{a}$, 而 $\pi_2(\alpha) = -\sqrt{a}$. 令 $Q_i = \pi_i^{-1}(R^2)$, $i = 1, 2$, 则 Q_1 和 Q_2 是正锥 P 在 $F(\alpha)$ 上的全部拓展, 使得 $\alpha \in Q_1$, 而 $-\alpha \in Q_2$. 证毕.

§2.4 Sturm 定理

在上节中, 定理 2.3.3 给出了一个判定系数在序域中的多项式在实闭包中的相异根个数的法则. 在本节中, 我们再给出另一个判定多项式的实根个数的方法, 这一方法是由 Sturm 首先发现的, 故关于该方法的描述被称作 Sturm 定理. 当然, Sturm 定理发现于实域理论的创立之先, 其原始形式仅针对于特殊实闭域 —— 实数域. 在本节的讨论中, 我们先建立更一般的 Sylvester-Sturm 定理, 以致于 Sturm 定理可作为其推论而得到.

在本节中, 下列定义对于后面的讨论起着根本性作用.

定义 2.4.1 设 F 是一个序域, $f(x)$, $g(x)$ 是 $F[x]$ 中非零多项式. 多项式 $f(x)$ 和 $g(x)$ 的 Sturm 序列是指 $F[x]$ 中这样一个多项式序列 $(f_0, f_1, \cdots, f_k)$, 使得下列条件成立:

(1) $f_0 = f$, $f_1 = g$;

(2) $f_{i-2} = f_{i-1}q_i - f_i$, 其中 $q_i \in F[x]$, 且 f_i 的次数低于 f_{i-1} 的次数, $i = 2, \cdots, k$;

(3) f_k 是 f 和 g 的一个最大公因式.

由上面定义可知, 借助于多项式的带余除法, 我们可以得到 $F[x]$ 中任意两个多项式的 Sturm 序列. 为节省符号, 对于一个序域 $(F, \leqslant)$ 的实闭包 R, R 的惟一序今后将仍用 $\leqslant$ 表示.

定义 2.4.2 设 $(F, \leqslant)$ 是一个序域, R 是它的实闭包, $(a_0, a_1, \cdots, a_k)$ 是由 R

中元素组成的一个序列，其中 $a_0 \neq 0$. 如果序列 $(a_0, a_1, \cdots, a_k)$ 中全部非零元素按原来顺序排列如次： $a_{j_1}, a_{j_2}, \cdots, a_{j_s}$, 其中 $0 = j_1 < j_2 < \cdots < j_s \leqslant k$, 则如下足标集

$$\{j_i \mid a_{j_i} a_{j_{i+1}} < 0\}$$

中元素个数称作序列 $(a_0, a_1, \cdots, a_k)$ 的变号数，且记作 $v(a_0, a_1, \cdots, a_k)$.

如果 $(f_0, f_1, \cdots, f_k)$ 是 $F[x]$ 中非零多项式 f 和 g 的 Sturm 序列，且 $a \in R$, 使得 $f(a) \neq 0$, 那么序列 $(f_0(a), f_1(a), \cdots, f_k(a))$ 的变号数记作 $v(f, g; a)$.

引理 2.4.1 设 R 是一个实闭域， $f(x) \in R[x]$. 若 $a, b \in R$, 且 $a < b$, 则有 $c \in]a, b[$, 使得 $f'(c) = \dfrac{f(a) - f(b)}{a - b}$.

证明 令 $g(x) = f(x) - f(b) - \dfrac{f(a) - f(b)}{a - b}(x - b)$, 则 $g(a) = g(b) = 0$. 由定理 2.1.7 知，有 $c \in]a, b[$, 使得 $g'(c) = 0$, 即有 $f'(c) = \dfrac{f(a) - f(b)}{a - b}$. 证毕.

引理 2.4.2 设 R 是一个实闭域， $f(x) \in R[x]$, $a, b \in R$, 且 $a < b$. 若 $f(x)$ 在开区间 $]a, b[$ 内恒取正（负）值，则 $f(x)$ 在闭区间 $[a, b]$ 上严格地单调递增 (递减).

证明 不妨设 $f(x)$ 在 $]a, b[$ 内恒取正值. 对于 $\alpha, \beta \in [a, b]$, 其中 $\alpha < \beta$, 由引理 2.4.1 知，有 $c \in]\alpha, \beta[\subseteq]a, b[$, 使得 $\dfrac{f(\alpha) - f(\beta)}{\alpha - \beta} = f'(c) > 0$. 由此可知， $f(\alpha) < f(\beta)$. 证毕.

由上面的引理 2.4.2, 我们可以建立适合实闭域的最值定理如下.

命题 2.4.3 设 R 是一个实闭域， $f(x) \in R[x]$. 若 $a, b \in R$, 且 $a < b$, 则有 $f(x)$ 在闭区间 $[a, b]$ 上有最大值和最小值，即有 $c, d \in [a, b]$, 使得对于每个 $z \in [a, b]$, $f(d) \leqslant f(z) \leqslant f(c)$.

证明 若 $f(x) \in R$, 则命题显然成立. 设 $f(x) \notin R$, 则 $f'(x)$ 是 $R[x]$ 中非零多项式. 记 $u_1, \cdots, u_s$ 是 $f'(x)$ 在 $]a, b[$ 内的全部根，且令 $f(c)$ 和 $f(d)$ 分别为序列: $f(a), f(b), f(u_1), \cdots, f(u_s)$ 中的最大元和最小元. 由引理 2.4.2 易知， $f(c)$ 和 $f(d)$ 分别是 $f(x)$ 在闭区间 $[a, b]$ 上的最大值和最小值. 证毕.

引理 2.4.4 设 $(F, \leqslant)$ 是一个实闭包为 R 的序域， $f(x)$ 和 $g(x)$ 是 $F[x]$ 中两个互素的多项式， $(f_0, f_1, \cdots, f_k)$ 是 $f(x)$ 和 $g(x)$ 的 Sturm 序列. 若 $a, b \in R$, 使得 $a < b$, $f_i(a) f_i(b) \neq 0$, $i = 0, 1, \cdots, k$, 且乘积 $f_0 f_1 \cdots f_k$ 在开区间 $]a, b[$ 内至多有一个根，则当 $f_0(a)$ 和 $f_0(b)$ 具有相同符号时， $v(f, g; a) = v(f, g; b)$.

证明 由条件可知， f_k 是 F 中非零元，且对于 $i = 1, \cdots, k$, f_{i-1} 和 f_i 是互素的.

由于 $f_0(a)$ 和 $f_0(b)$ 有相同符号，从而有最大足标 m, $0 \leqslant m \leqslant k$, 使得序列 $(f_0(a), \cdots, f_m(a))$ 和 $(f_0(b), \cdots, f_m(b))$ 具有相同的变号数. 我们的目标是证明

$m=k$.

假设 $m<k$. 当 $f_{m+1}(a)$ 与 $f_{m+1}(b)$ 的符号相同时， $f_m(a)$ 与 $f_m(b)$ 的符号必相反；否则序列 $(f_0(a),\cdots,f_m(a),f_{m+1}(a))$ 和 $(f_0(b),\cdots,f_m(b),f_{m+1}(b))$ 具有相同的变号数. 此时必有 $m>1$. 由中间值定理， $f_m(x)$ 在 $]a,b[$ 中有根 α. 由于 f_{m-1} 和 f_{m+1} 均与 $f_m(x)$ 互素，从而 α 不是它们的根. 于是 f_{m-1} 和 f_{m+1} 在 $]a,b[$ 中无根. 于是 $f_{m-1}(a)$, $f_{m-1}(b)$ 与 $f_{m-1}(\alpha)$, 而 $f_{m+1}(a)$, $f_{m+1}(b)$ 与 $f_{m+1}(\alpha)$ 具有相同符号. 由于 $f_{m-1}=q_{m+1}f_m-f_{m+1}$, 从而 $f_{m-1}(\alpha)=-f_{m+1}(\alpha)$. 这表明： $f_{m-1}(a)$ 和 $f_{m+1}(a)$ 具有相反符号，且 $f_{m-1}(b)$ 和 $f_{m+1}(b)$ 具有相反符号. 此时易见，序列 $(f_0(a),\cdots,f_m(a),f_{m+1}(a))$ 和 $(f_0(b),\cdots,f_m(b),f_{m+1}(b))$ 具有相同的变号数，矛盾于 m 的选取. 当 $f_{m+1}(a)$ 与 $f_{m+1}(b)$ 具有相反的符号时，必定有 $m+1<k$, 因为 $f_k\in\dot{F}$. 通过类似于上面的讨论可知，序列 $(f_0(a),\cdots,f_m(a),f_{m+1}(a),f_{m+2}(a))$ 和 $(f_0(b),\cdots,f_m(b),f_{m+1}(b),f_{m+2}(b))$ 具有相同的变号数，矛盾. 因此， $m=k$. 证毕.

在下面，我们将建立 Sylvester-Sturm 定理. 为叙述简明，我们需要引进一些如下记号.

设 (F,P) 是一个实闭包为 R 的序域， $f(x)$ 和 $g(x)$ 是 $F[x]$ 中非零多项式, a, $b\in R$, 使得 $a<b$, 则集合 $\{\alpha\in R\mid a<\alpha<b,\ f(\alpha)=0,\ \text{而}\ g(\alpha)>0\}$ 与集合 $\{\alpha\in R\mid a<\alpha<b,\ f(\alpha)=0,\ \text{而}\ g(\alpha)<0\}$ 的元素个数分别记作 $N_a^b(f,g>0)$ 和 $N_a^b(f,g<0)$. 显然，对于 $c\in R$, 其中 $a<c<b$ 且 $f(c)\neq0$, $N_a^b(f,g>0)=N_a^c(f,g>0)+N_c^b(f,g>0)$, 且 $N_a^b(f,g<0)=N_a^c(f,g<0)+N_c^b(f,g<0)$.

定理 2.4.5 (Sylvester-Sturm 定理) 设 (F,P) 是一个序域， R 是它的实闭包, $f(x)$ 和 $g(x)$ 是 $F[x]$ 中非零多项式. 若 a, $b\in R$, 使得 $a<b$, 且 $f(a)f(b)\neq0$, 则 $N_a^b(f,g>0)-N_a^b(f,g<0)=v(f,f'g;a)-v(f,f'g;b)$.

证明 设 $(f_0,f_1,\cdots,f_k)$ 是多项式 $f(x)$ 和 $f'(x)g(x)$ 的 Sturm 序列. 令 $g_i=\dfrac{f_i}{f_k}$, $i=0,1,\cdots,k$. 易知， $(g_0,g_1,\cdots,g_k)$ 是互素多项式 g_0 和 g_1 的 Sturm 序列，使得 $v(f,f'g;a)=v(g_0,g_1;a)$, 且 $v(f,f'g;b)=v(g_0,g_1;b)$. 此外可断言：对于 $\alpha\in R$, $g_0(\alpha)=0$, 当且仅当 $f(\alpha)=0$, 但 $g(\alpha)\neq0$. 事实上，若用 s 和 t 分别表示 α 作为 $f(x)$ 和 $g(x)$ 的根的重数，其中 $s>0$, $t\geqslant0$, 则 α 是 $f'(x)g(x)$ 的 $s+t-1$ 重根. 于是， α 作为 $f_k(x)$ 的根的重根为 $\min\{s,s+t-1\}$. 从而 $t=0$, 当且仅当 $s-\min\{s,s+t-1\}=1$, 即 α 是 g_0 的 (单) 根.

将多项式的乘积 $f_0f_1\cdots f_k$ 在 R 中的全部相异根排列如下：

$$\alpha_1<\alpha_2<\cdots<\alpha_n.$$

令 $a_i=\dfrac{1}{2}(\alpha_i+\alpha_{i+1})$, $i=1,\cdots,n-1$, 则有

$$a := a_0 < \alpha_1 < a_1 < \alpha_2 < \cdots < a_{n-1} < \alpha_n < a_n := b.$$

考察每个开区间 $]a_{i-1}, a_i[$, $i = 1, \cdots, n$. 当 $g_0(\alpha_i) \neq 0$ 时, g_0 在 $]a_{i-1}, a_i[$ 中无根. 由中间值定理知, $g_0(a_{i-1})$ 和 $g_0(a_i)$ 具有相同符号. 由引理 2.4.4 知, $v(g_0, g_1; a_{i-1}) = v(g_0, g_1; a_i)$, 即 $v(f, f'g; a_{i-1}) = v(f, f'g; a_i)$. 此时有

$$v(f, f'g; a_{i-1}) - v(f, f'g; a_i) = 0 = 0 - 0 = N_{a_{i-1}}^{a_i}(f, g > 0) - N_{a_{i-1}}^{a_i}(f, g < 0).$$

现设 $g_0(\alpha_i) = 0$, 则 $g(\alpha_i) \neq 0$, 且 $g_1(\alpha_i) \neq 0$. 从而 g_1 在 $]a_{i-1}, a_i[$ 中无根, 即知 $g_1(a_{i-1})$ 和 $g_1(a_i)$ 的符号相同. 注意到 $(g_1, \cdots, g_k)$ 是多项式 g_1 和 g_2 的 Sturm 序列, 而且 g_1 和 g_2 互素. 由引理 2.4.4 知, 序列 $(g_1(a_{i-1}), \cdots, g_k(a_{i-1}))$ 和 $(g_1(a_i), \cdots, g_k(a_i))$ 具有相同的变号数. 这表明: 序列 $(f_1(a_{i-1}), \cdots, f_k(a_{i-1}))$ 和 $(f_1(a_i), \cdots, f_k(a_i))$ 具有相同的变号数.

对于 $g(\alpha_i)$ 的符号, 分情况讨论.

(1) $g(\alpha_i) > 0$. 由于 $g(x)$ 在闭区间 $[a_{i-1}, a_i]$ 上无根, 从而必有 $g(a_{i-1}) > 0$, 且 $g(a_i) > 0$. 注意到 $f'(x)$ 在开区间 $]a_{i-1}, \alpha_i[$ 和 $]\alpha_i, a_i[$ 内都无根, 从而有如下四种可能:

(1.1) $f'(x)$ 在开区间 $]a_{i-1}, \alpha_i[$ 和 $]\alpha_i, a_i[$ 内都取正值. 此时, 由引理 2.4.2 可知, $f(a_{i-1}) < 0$, 而 $f(a_i) > 0$.

(1.2) $f'(x)$ 在开区间 $]a_{i-1}, \alpha_i[$ 和 $]\alpha_i, a_i[$ 内都取负值. 此时有 $f(a_{i-1}) > 0$, 而 $f(a_i) < 0$.

(1.3) $f'(x)$ 在开区间 $]a_{i-1}, \alpha_i[$ 和 $]\alpha_i, a_i[$ 内分别取正值和负值. 此时, 显然有 $f(a_{i-1}) < 0$ 且 $f(a_i) < 0$.

(1.4) $f'(x)$ 在开区间 $]a_{i-1}, \alpha_i[$ 和 $]\alpha_i, a_i[$ 内分别取负值和正值. 此时, 显然有 $f(a_{i-1}) > 0$ 且 $f(a_i) > 0$.

在上面四种可能的情况下, 都有 $f_0(a_{i-1})f_1(a_{i-1}) < 0$, 但 $f_0(a_i)f_1(a_i) > 0$. 因而有, $v(f, f'g; a_{i-1}) - v(f, f'g; a_i) = 1 = 1 - 0 = N_{a_{i-1}}^{a_i}(f, g > 0) - N_{a_{i-1}}^{a_i}(f, g < 0)$.

(2) $g(\alpha_i) < 0$. 类似可得 $v(f, f'g; a_{i-1}) - v(f, f'g; a_i) = -1 = 0 - 1 = N_{a_{i-1}}^{a_i}(f, g > 0) - N_{a_{i-1}}^{a_i}(f, g < 0)$.

综上所述, 我们总有 $N_{a_{i-1}}^{a_i}(f, g > 0) - N_{a_{i-1}}^{a_i}(f, g < 0) = v(f, f'g; a_{i-1}) - v(f, f'g; a_i)$. 由此有 $N_a^b(f, g > 0) - N_a^b(f, g < 0) = \sum_{i=1}^{n}(N_{a_{i-1}}^{a_i}(f, g > 0) - N_{a_{i-1}}^{a_i}(f, g < 0)) = \sum_{i=1}^{n}(v(f, f'g; a_{i-1}) - v(f, f'g; a_i)) = v(f, f'g; a) - v(f, f'g; b)$. 证毕.

由上面定理, 立即可推出下面的 Sturm 定理.

定理 2.4.6 设 (F, P) 是一个实闭包为 R 的序域, $f(x)$ 是 $F[x]$ 中非零多项式, $a, b \in R$, 使得 $a < b$, 且 $f(a)f(b) \neq 0$, 则 $f(x)$ 在 R 中大于 a 且小于 b 的相异

根的总数等于 $v(f,f';a)-v(f,f';b)$.

证明 只需在定理 2.4.5 中，取 $g=1$ 即可.

推论 1 设 $(F,\leqslant)$ 是一个序域， $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n\in F[x]$, 其中 $a_0\neq 0$, 则 $f(x)$ 在 $(F,\leqslant)$ 的实闭包中的相异根个数等于 $v(f,f';-M)-v(f,f',M)$, 这里 $M=1+\sum\limits_{i=1}^{n}|\frac{a_i}{a_0}|$.

证明 设 R 是 $(F,\leqslant)$ 的实闭包，且 α 是 $f(x)$ 在 R 中任意一个根. 通过引理 1.2.2 的类似证明，可知 $-M<\alpha<M$. 由此知， $f(x)$ 在 R 中全部根都在 $]-M,M[$ 中. 从而由定理 2.4.6 即得结论. 证毕.

推论 2 设 $(F,\leqslant)$ 是一个实闭包为 R 的序域， $f(x)$ 和 $g(x)$ 是 $F[x]$ 中非零多项式， $(f_0,f_1,\cdots,f_k)$ 是 $f(x)$ 和 $f'g(x)$ 的 Sturm 序列. 若 a_i 为 f_i 的首项系数，而 b_i 为 $f_i(-x)$ 的首项系数， $i=0,1,\cdots,k$, 则集合 $\{\alpha\in R\mid f(\alpha)=0, 而\ g(\alpha)>0\}$ 与集合 $\{\alpha\in R\mid f(\alpha)=0, 而\ g(\alpha)<0\}$ 的元素个数之差等于序列 $(b_0,b_1,\cdots,b_k)$ 与 $(a_0,a_1,\cdots,a_k)$ 的变号数之差.

证明 由上面的推论 1 知，存在 F 中正元素 M, 使得多项式乘积 $f_0f_1\cdots f_k$ 在 R 中全部根都属于 R 的开区间 $]-M,M[$. 由定理 2.4.5 知，只须证明： a_i 和 $f_i(M)$, 而 b_i 和 $f_i(-M)$ 具有相同的符号， $i=0,1,\cdots,k$.

假若对于某个 $j\in\{0,1,\cdots,k\}$, $a_jf_j(M)<0$. 设 $f_j(x)=a_jx^d+c_1x^{d-1}+\cdots+c_d$, 其中 $c_1,\cdots,c_d\in F$, 则 $h(0)h(M^{-1})=M^{-d}a_jf_j(M)<0$, 这里 $h(x)=a_j+c_1x+\cdots+c_dx^d$. 由中间值定理知，有 $\beta\in]0,M^{-1}[$, 使得 $h(\beta)=0$. 此时易知， $f_j(\beta^{-1})=0$ 但 $M<\beta^{-1}$, 矛盾. 因而， $a_if_i(M)>0$, $i=0,1,\cdots,k$. 同理， $b_if_i(-M)>0$, $i=0,1,\cdots,k$. 证毕.

作为多项式的正根个数的一个简单估计，可以建立如下命题，这一命题常被人称作 Descartes 引理.

命题 2.4.7 设 $(F,\leqslant)$ 是一个实闭包为 R 的序域， $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n\in F[x]$, 其中 $a_0\neq 0$, 则 $f(x)$ 在 R 中正根个数不超过序列 $(a_0,a_1,\cdots,a_n)$ 的变号数，且 $f(x)$ 在 R 中正根个数和序列 $(a_0,a_1,\cdots,a_n)$ 的变号数具有相同的奇偶性，这里正重根个数按重数计算.

证明 首先，对 n 施用归纳法，证明前一结论： $f(x)$ 在 R 中正根个数不超过序列 $(a_0,a_1,\cdots,a_n)$ 的变号数. 当 $n=1$ 时，该结论显然成立. 假定该结论对于次数为 $n-1$ 的多项式成立. 现考虑如命题所示的 n 次多项式 $f(x)$, 且记 m 为 $f(x)$(在 R 中) 的正根个数. 如若 $a_n=0$, 则 $f(x)$ 的正根个数等于 $a_0x^{n-1}+a_1x^{n-2}+\cdots+a_{n-1}$ 的正根个数. 由归纳假定， $f(x)$ 的正根个数不超过 $v(a_0,a_1,\cdots,a_{n-1})$, 即不超过 $v(a_0,a_1,\cdots,a_{n-1},a_n)$. 下设 $a_n\neq 0$, 且令 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-q}x^q+a_n$, 其中 $1\leqslant q\leqslant n$, 且 $a_{n-q}\neq 0$. 若 $m=1$, 即 $f(x)$ 只有一个正根，则易知 $(a_0,a_1,\cdots,a_n)$

中至少有两个非零元素具有相反符号，即 $v(a_0, a_1, \cdots, a_n) \geqslant 1 = m$. 进一步设 $m > 1$. 由定理 2.1.7 可知，$f'(x)$ 在 R 中至少有 $m-1$ 个正根分别介于 $f(x)$ 的各对相邻的正根之间或为 $f(x)$ 的重根. 令 c 是 $f'(x)$ 的最小正根. 现考虑如下两种情况：

(1) $a_{n-q}a_n > 0$. 由于 $f'(x)$ 在开区间 $]0, c[$ 内无根，从而由中间值定理知，$f'(x)$ 在 $]0, c[$ 内的值保持相同符号. 注意到，$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \cdots + qa_{n-q}x^{q-1}$. 此时易证：对于充分小的 $\epsilon \in]0, c[$, $f'(\epsilon)$ 与 $f'(x)$ 的尾项系数 qa_{n-q} 具有相同符号，即与 a_n 具有相同符号. 因而，$a_nf'(x)$ 在 $]0, c[$ 上恒取正值. 由引理 2.4.2 知，$a_nf(x)$ 在 $[0, c]$ 上是严格地单调递增的. 由于 $a_nf(0) = a_n^2 > 0$, 从而 $a_nf(x)$ 即 $f(x)$ 在 $[0, c]$ 上无根. 这表明：$f'(x)$ 的这个根 c 既不介于 $f(x)$ 的任何一对相邻的正根之间，又不是 $f(x)$ 的重根. 此外，除 c 外，$f'(x)$ 在 R 中有 $m-1$ 个正根，其中每个根都介于 $f(x)$ 的两个正根之间或为 $f(x)$ 的重根. 因而，$f'(x)$ 至少有 m 个在 R 中的正根，即 $f(x)$ 在 R 中的正根个数不超过 $f'(x)$ 在 R 中的正根个数. 由归纳假设，$f(x)$ 在 R 中的正根个数不超过序列 $(na_0, (n-1)a_1, \cdots, qa_{n-q})$ 的变号数，即序列 $(a_0, a_1, \cdots, a_{n-q}, \cdots, a_n)$ 的变号数.

(2) $a_{n-q}a_n < 0$. 此时，$v(a_0, a_1, \cdots, a_{n-q}) = v(a_0, a_1, \cdots, a_{n-q}, \cdots, a_n) - 1$. 根据定理 2.1.7 可知，多项式 $f'(x)$ 在 R 中至少有 $m-1$ 个正根分别介于 $f(x)$ 的各对相邻的正根之间或为 $f(x)$ 的重根. 由归纳假定有

$$m - 1 \leqslant v(a_0, a_1, \cdots, a_{n-q}) = v(a_0, a_1, \cdots, a_{n-q}, \cdots, a_n) - 1.$$

从而

$$m \leqslant v(a_0, a_1, \cdots, a_{n-q}, \cdots, a_n).$$

因而，前一结论对于 n 次多项式也成立. 由归纳法原理，命题中前一结论获证.

现在，我们来证明命题中后一结论. 设 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-q}x^q$, 其中 $0 \leqslant q \leqslant n$, 且 $a_{n-q} \neq 0$. 记 $f(x)$ 在代数闭域 $R[\sqrt{-1}]$ 中的全部非零根为：

$$b_1, \cdots, b_m; \quad -c_1, \cdots, -c_s;$$

$$d_1 + e_1\sqrt{-1},\ d_1 - e_1\sqrt{-1},\ \cdots,\ d_t + e_t\sqrt{-1},\ d_t - e_t\sqrt{-1},$$

其中 $b_i, c_j, e_k, d_k \in R$, $b_i > 0$, $i = 1, \cdots, m$; $c_j > 0$, $j = 1, \cdots, s$; $e_k \neq 0$, $k = 1, \cdots, t$, 且 $m + s + 2t = n - q$.

由多项式的根与系数的关系，我们有

$$(-1)^s \prod_{i=1}^{m} a_i \prod_{j=1}^{s} b_j \prod_{k=1}^{t} (d_k^2 + e_k^2) = (-1)^{n-q} \frac{a_0}{a_{n-q}}.$$

若序列 $(a_0, a_1, \cdots, a_{n-q})$ 的变号数为偶数，则 a_0 和 a_{n-q} 的符号相同，即 $\dfrac{a_0}{a_{n-q}} > 0$. 由此有，$(-1)^m = (-1)^{m+2t} = (-1)^{n-q-s} = 1$. 这表明：$f(x)$ 在 R 中的正根个数 m 是偶数. 同理可知，当序列 $(a_0, a_1, \cdots, a_{n-q})$ 的变号数为奇数时，a_0 和 a_{n-q} 的符号相反，即 $\dfrac{a_0}{a_{n-q}} < 0$. 此时可证，$f(x)$ 在 R 中的正根个数是奇数. 至此，定理获证.

§2.5 Sylvester 矩阵和多项式的判别系统

在 §2.3 中，为证明序域的实闭包的惟一性，我们建立了著名的 Sylvester 定理 (定理 2.3.3), 这一定理可用来判定序域上的多项式是否在实闭包中有根. 然而，由于 Sylvester 定理所涉及的二次型的系数不是直接通过多项式的系数给出，从而在实际应用 Sylvester 定理中感到不方便. 在本节中，我们将在 Sylvester 定理和 Sturm 定理的基础上作进一步的讨论，从而获得更深刻且应用方便的结果.

在本节中，始终设 (F, P) 是一个序域，R 是一个实闭域，使得 $P \subseteq R^2$, 则由定理 2.1.3 知，$R(\sqrt{-1})$ 是包含 F 的代数闭域. 设 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ 是 F 上一个 n 次多项式，其中 $n > 0$ 且 $a_0 \neq 0$, 则 $f(x)$ 在 $R(\sqrt{-1})[x]$ 中可分解为

$$f(x) = a_0(x - \alpha_1)\cdots(x - \alpha_n),$$

其中 $\alpha_i \in R(\sqrt{-1}), i = 1, \cdots, n$.

对于每个非负整数 k, 记 $\sigma_k := \sum_{i=1}^{n} \alpha_i^k$. 根据 §2.3 的讨论，我们可以得到 F 上的如下二次型：

$$\rho_f := \sum_{i=1}^{n}\sum_{j=1}^{n} \sigma_{i+j-2}x_ix_j.$$

由 Sylvester 定理及其证明可知，多项式 $f(x)$ 在 R 中的相异根的个数等于二次型 ρ_f 的符号差 $\mathrm{sgn}_P(\rho_f)$, 而 $f(x)$ 在 $R(\sqrt{-1})$ 中的相异根的个数等于二次型 ρ_f 的秩.

用 A_f 表示二次型 ρ_f 的矩阵，即 $A_f = (\sigma_{i+j-2})_{n\times n}$. 记 $\alpha_1, \cdots, \alpha_r$ 是 $f(x)$ 在 R 中的全部相异根，且它们的重数分别为 $m_1, \cdots, m_r$. 同时，设 $f(x)$ 在 $R(\sqrt{-1})$ 中但不在 R 内且成对出现的共轭根为 $\beta_1, \bar{\beta}_1; \cdots, \beta_t, \bar{\beta}_t$. 令 M_v 为根 β_v 和 $\bar{\beta}_v$ 的相同重数，$v = 1, \cdots, t$.

考虑 F 上的如下 $r + 2t$ 元二次型：

$$g = \sum_{i=1}^{r+2t}\sum_{j=1}^{r+2t}\left[\sum_{u=1}^{r} m_u \alpha_u^{i+j-2} + \sum_{v=1}^{t}(\beta_v^{i+j-2} + \bar{\beta}_v^{i+j-2})\right] x_i x_j$$
$$= \sum_{u=1}^{r} m_u \left(\sum_{i=1}^{r+2t} \alpha_u^{i-1} x_i\right)^2 + \sum_{v=1}^{t} M_v \left[\left(\sum_{i=1}^{r+2t} \beta_v^{i-1} x_i\right)^2 + \left(\sum_{i=1}^{r+2t} \bar{\beta}_v^{i-1} x_i\right)^2\right].$$

令

$$y_u = \sum_{i=1}^{r+2t} \alpha_u^{i-1} x_i,\ u = 1, \cdots, r;$$
$$y_{r+2v-1} = \sum_{i=1}^{r+2t} \frac{1}{2}(\beta_v^{i-1} + \bar{\beta}_v^{i-1}) x_i,\ v = 1, \cdots, t;$$
$$y_{r+2v} = \sum_{i=1}^{r+2t} \frac{\sqrt{-1}}{2}(\bar{\beta}_v^{i-1} - \beta_v^{i-1}) x_i,\ v = 1, \cdots, t.$$

显然，上面的关系式给出了 R 上一个非退化线性替换. 通过这个线性替换，ρ_f 化成如下标准型：

$$\rho_f = \sum_{u=1}^{r} m_u y_u^2 + \sum_{v=1}^{t} M_v (y_{r+2v-1}^2 - y_{r+2v}^2).$$

由此可见，二次型 g 是非退化的. 因而，矩阵 A_f 的第 $r+2t$ 个顺序主子式不为零. 由于 A_f 的秩恰为 $r+2t$, 因而从 A_f 的第 $r+2t+1$ 个顺序主子式开始，后面的顺序主子式全为零.

通过多项式 f 的系数构造如下上三角矩阵：

$$C = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ 0 & a_0 & a_1 & \cdots & a_{n-2} \\ 0 & 0 & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & a_0 \end{pmatrix}.$$

记 b_{ij} 为对称矩阵 $C^t A_f C$ 中第 i 行第 j 列元素，则显然有

$$b_{ij} = \sum_{k=0}^{j-1}\sum_{\ell=0}^{i-1} a_{i-1-\ell}\sigma_{k+\ell} a_{j-1-k},\ i, j = 1, \cdots, n.$$

由此有 $b_{11} = na_0^2$, 且 $b_{21} = (n-1)a_0 a_1$. 当 $i \geqslant j \geqslant 2$ 时，借助于牛顿公式

$\sum_{i=1}^{k} a_{k-i}\sigma_i = -ka_k (k = 1, \cdots, n)$, 我们有

$$\begin{aligned}
b_{ij} &= \sum_{k=0}^{j-1} a_{j-1-k}\left(\sum_{\ell=0}^{i-1} a_{i-1-\ell}\sigma_{k+\ell}\right) \\
&= a_{j-1}\left(\sum_{\ell=0}^{i-1} a_{i-1-\ell}\sigma_\ell\right) \\
&\quad + a_{j-2}\left(\sum_{\ell=0}^{i-1} a_{i-1-\ell}\sigma_{1+\ell}\right) + \sum_{k=2}^{j-1} a_{j-1-k}\left(\sum_{\ell=0}^{i-1} a_{i-1-\ell}\sigma_{k+\ell}\right) \\
&= (n-i+1)a_{i-1}a_{j-1} - ia_i a_{j-2} \\
&\quad + \sum_{k=2}^{j-1} a_{j-1-k}\left(\sum_{\ell=1-k}^{i-1} a_{i-1-\ell}\sigma_{k+\ell} - \sum_{\ell=1-k}^{-1} a_{i-1-\ell}\sigma_{k+\ell}\right) \\
&= (n-i+1)a_{i-1}a_{j-1} - ia_i a_{j-2} \\
&\quad - \sum_{k=2}^{j-1} a_{j-1-k}\left((k+i-1)a_{k+i-1} + \sum_{\ell=1-k}^{-1} a_{i-1-\ell}\sigma_{k+\ell}\right) \\
&= (n-i+1)a_{i-1}a_{j-1} - ia_i a_{j-2} \\
&\quad - \sum_{k=2}^{j-1}(k+i-1)a_{j-1-k}a_{k+i-1} - \sum_{k=2}^{j-1} a_{j-1-k}\left(\sum_{\ell=1-k}^{-1} a_{i-1-\ell}\sigma_{k+\ell}\right) \\
&= (n-i+1)a_{i-1}a_{j-1} - ia_i a_{j-2} \\
&\quad - \sum_{k=2}^{j-1}(k+i-1)a_{j-1-k}a_{k+i-1} - \sum_{k=1}^{j-2} a_{j-2-k}\left(\sum_{\ell=-k}^{-1} a_{i-1-\ell}\sigma_{\ell+k+1}\right) \\
&= (n-i+1)a_{i-1}a_{j-1} - ia_i a_{j-2} \\
&\quad - \sum_{k=2}^{j-1}(k+i-1)a_{j-1-k}a_{k+i-1} - \sum_{k=1}^{j-2}\sum_{\ell=1}^{k} a_{i-1+\ell}\sigma_{k+1-\ell} \\
&= (n-i+1)a_{i-1}a_{j-1} - ia_i a_{j-2} \\
&\quad - \sum_{k=2}^{j-1}(k+i-1)a_{j-1-k}a_{k+i-1} - \sum_{\ell=1}^{j-2} a_{i-1+\ell}\left(\sum_{k=\ell}^{j-2} a_{j-2-k}\sigma_{k+1-\ell}\right) \\
&= (n-i+1)a_{i-1}a_{j-1} - ia_i a_{j-2} \\
&\quad - \sum_{k=2}^{j-1}(k+i-1)a_{j-1-k}a_{k+i-1} + \sum_{\ell=1}^{j-2}(j-\ell-1)a_{i-1+\ell}a_{j-\ell-1} \\
&= (n-i+1)a_{i-1}a_{j-1} - \sum_{m=0}^{j-2}(i+j-2-2m)a_m a_{i+j-2-m}.
\end{aligned}$$

定义 2.5.1 如上所得的对称矩阵 $C^t A_f C$ 称作多项式 f 的 Bezout 矩阵，且记作 Bezout(f).

根据上面的计算公式, 容易得到矩阵 Bezout(f) 的所有元素. 显然, 矩阵 Bezout(f) 和 A_f 合同, 且两矩阵的第 k 个顺序主子式仅相差一个正因子 a_0^{2k}, $k=1,\cdots,n$. 由 Sylvester 定理和上面的讨论, 立即有下面的结论.

定理 2.5.1 所设同上, 且 r 为对称矩阵 Bezout(f) 的秩, 则下面的事实成立:

(1) $f(x)$ 在 R 中的相异根的个数等于对称矩阵 Bezout(f) 的符号差;

(2) $f(x)$ 在 $R(\sqrt{-1})$ 中的相异根的个数等于秩 r;

(3) 矩阵 Bezout(f) 的第 r 个顺序主子式不为零, 但第 k 个顺序主子式为零, 只要 $k>r$.

用上面的定理 2.5.1 来考察多项式的实根, 既要计算出 Bezout 矩阵中全部元素, 又要对 Bezout 矩阵进行合同变换以求出符号差. 这样, 不仅带来计算和记忆上的困难, 而且在对有参数的多项式的 Bezout 矩阵进行合同变换时将出现许多繁杂的情形. 下面介绍另一种与多项式有关的矩阵 ——Sylvester 矩阵, 只需计算该矩阵的一些子式, 即可获知多项式的实根的有关信息.

对于域 F 上的如下两个多项式:

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n,$$
$$g(x)=b_1x^{n-1}+b_2x^{n-2}+\cdots+b_n,$$

其中 $n>0$ 且 $a_0\neq 0$, 我们可构造如下三类矩阵:

$$S(f,g;k):=\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_n & & & & \\ 0 & b_1 & b_2 & \cdots & b_n & & & & \\ & a_0 & a_1 & a_2 & \cdots & a_n & & & \\ & 0 & b_1 & b_2 & \cdots & b_n & & & \\ & & \vdots & \vdots & & \vdots & & & \\ & & 0 & a_0 & a_1 & a_2 & \cdots & a_n \\ & & & 0 & b_1 & b_2 & \cdots & b_n \end{pmatrix}_{2k\times(n+k)},$$

$$S(g,f;k):=\begin{pmatrix} 0 & b_1 & b_2 & \cdots & b_n & & & & \\ a_0 & a_1 & a_2 & \cdots & a_n & & & & \\ & 0 & b_1 & b_2 & \cdots & b_n & & & \\ & a_0 & a_1 & a_2 & \cdots & a_n & & & \\ & & & \vdots & & \vdots & & & \\ & & & 0 & b_1 & b_2 & \cdots & b_n \\ & & & a_0 & a_1 & a_2 & \cdots & a_n \end{pmatrix}_{2k\times(n+k)},$$

$$T(f;\ell,s) := \begin{pmatrix} a_0 & a_1 & \cdots & a_n & 0 & 0 & 0 & 0 & \cdots & 0 \\ & a_0 & a_1 & \cdots & a_n & 0 & 0 & 0 & \cdots & 0 \\ & & & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ & & & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \end{pmatrix}_{\ell\times(n+\ell+s)},$$

这里 $k,\ell\in\mathbb{N}$, 而 $s\in\mathbb{N}\cup\{0\}$.

在下面, 矩阵中两行互换以及某行乘以 -1 的变换将称作第一类初等行变换; 而矩阵中某行乘以 F 中元素再加到另一行的变换将称作第二类初等行变换.

引理 2.5.2 设多项式 $f(x)$ 和 $g(x)$ 同上, $\delta=\deg f(x)-\deg g(x)$, 且有带余除式: $f(x)=q(x)g(x)-r(x)$, 其中 $q(x),\ r(x)\in F[x]$, 且 $\deg r(x)<m$, 则有下列事实:

(1) 当 $k\leqslant\delta$ 时, 经过 $\frac{1}{2}k(k-1)$ 次第一类初等行变换, 矩阵 $S(f,g;k)$ 可化为如下形式的矩阵:

$$\left(\begin{array}{c|c} \multicolumn{2}{c}{T(f;k,0)} \\ \hline O_{k\times\delta} & T(g;k,0) \end{array}\right).$$

(2) 当 $k>\delta$ 时, 经过 $\frac{1}{2}\delta(\delta-1)+2k-2\delta$ 次第一类初等行变换和若干次第二类初等行变换, 矩阵 $S(f,g;k)$ 可化为如下形式的矩阵:

$$\left(\begin{array}{c|c} \multicolumn{2}{c}{T(f;\delta,k-\delta)} \\ \hline O_{\delta\times\delta} & T(g;\delta,k-\delta) \\ \hline O_{2(k-\delta)\times2\delta} & S(g,r;k-\delta) \end{array}\right).$$

证明 (1) 设 $k\leqslant\delta$. 此时, 经过 $\frac{1}{2}k(k-1)$ 次第一类初等行变换, 将 $f(x)$ 的系数所在的行逐行上移, 即可化 $S(f,g;k)$ 为所求的矩阵形式.

(2) 设 $k>\delta$. 首先, 经过 $\frac{1}{2}\delta(\delta-1)$ 次第一类初等行变换, 逐行上移 $f(x)$ 的系数所在的前 $n-m-1$ 行 (第一行除外), 即可化 $S(f,g;k)$ 为如下矩阵:

$$\left(\begin{array}{c|c} \multicolumn{2}{c}{T(f;\delta,k-\delta)} \\ \hline O_{\delta\times\delta} & T(g;\delta,k-\delta) \\ \hline O_{\delta\times\delta} & S(f,g;k-\delta) \end{array}\right).$$

其次, 根据所给的带余除式 $-r(x)=f(x)-q(x)g(x)$, 经过若干次第二类初等行变换, 矩阵 $S(f,g;k)$ 可进一步化为如下矩阵:

$$\begin{pmatrix} \multicolumn{2}{c}{T(f;\delta,k-\delta)} \\ \hline O_{\delta\times\delta} & T(g;\delta,k-\delta) \\ \hline O_{\delta\times\delta} & S(-r,g;k-\delta) \end{pmatrix}.$$

再将矩阵后面 $2(k-\delta)$ 行分成相邻的 $k-\delta$ 对互换，最后把 $-r(x)$ 的系数所在的 $k-\delta$ 行分别乘以 -1, 即可化为所求的矩阵形式. 证毕.

定义 2.5.2 设多项式 $f(x)$ 和 $g(x)$ 同上. 如下 $2n\times 2n$ 矩阵称作 $f(x)$ 和 $g(x)$ 的 Sylvester 矩阵：

$$\mathrm{Sylvester}(f,g):=\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_n & & & & \\ 0 & b_1 & b_2 & \cdots & b_n & & & & \\ & a_0 & a_1 & a_2 & \cdots & a_n & & & \\ & 0 & b_1 & b_2 & \cdots & b_n & & & \\ & & & \vdots & & \vdots & & & \\ & & & a_0 & a_1 & a_2 & \cdots & a_n \\ & & & 0 & b_1 & b_2 & \cdots & b_n \end{pmatrix}_{2n\times 2n},$$

特别地，当 $g(x)$ 为 $f(x)$ 的微商 $f'(x)$ 时， $f(x)$ 和 $f'(x)$ 的 Sylvester 矩阵简称作 $f(x)$ 的 Sylvester 矩阵，且简记作 $\mathrm{Sylvester}(f)$.

显然， $\mathrm{Sylvester}(f,g)=S(f,g;n)$. 下面，我们将在引理 2.5.2 的基础上，探讨 Sylvester 矩阵的有关重要信息.

设多项式 $f(x)$ 和 $g(x)$ 同上， $\{f_0,f_1,\cdots,f_s\}$ 是 $f(x)$ 和 $g(x)$ 的 Sturm 序列，且令 $\delta_i=\deg f_i-\deg f_{i+1}$, $i=0,\cdots,s-1$. 用 D_{2k} 表示矩阵 $\mathrm{Sylvester}(f,g)$ 的第 $2k$ 个顺序主子式， $k=1,\cdots,n$. 此外，用 $D_{(2k,t)}$ 表示这样一个新矩阵的第 $2k$ 个顺序主子式，这样一个新矩阵是矩阵 $\mathrm{Sylvester}(f,g)$ 中第 $2k$ 列被第 $2k+t$ 列替换后所得的，其中 $0\leqslant t\leqslant 2n-k$, $k=1,\cdots,n$.

现在，我们可以建立下面的重要定理.

定理 2.5.3 所设同上，且设 c_i 为 f_i 的首项系数， $i=0,\cdots,s$, 则有

(1) 当 $k\notin\{\sum_{i=0}^{\ell}\delta_i\mid 0\leqslant\ell\leqslant s-1\}$ 时， $D_{2k}=0$.

(2) 当 $k=\sum_{i=0}^{\ell}\delta_i$ $(0\leqslant\ell\leqslant s-1)$ 时，

$$D_{2k}=(-1)^{e_k}(c_0c_1)^{\delta_0}(c_1c_2)^{\delta_1}\cdots(c_\ell c_{\ell+1})^{\delta_\ell},$$

其中 $e_k=\dfrac{1}{2}\sum_{i=0}^{\ell}\delta_i(\delta_i-1)$. 此时还有

$$f_{\ell+1}(x) = c_{\ell+1} \sum_{t=0}^{n-k} \frac{D_{(2k,t)}}{D_{2k}} x^{n-k-t}.$$

证明 显然, D_{2k} 是矩阵 $S(f,g;k)$ 的左边 $2k$ 级子式, 而 $D_{(2k,t)}$ 是矩阵 $S(f,g;k)$ 的左边 $2k-1$ 列和第 $2k+t$ 列所组成的 $2k$ 级子式，其中 $0 \leqslant t \leqslant 2n-k$.

由引理 2.5.2 知，矩阵 $S(f,g;k)$ 可通过初等行变换化成引理中所给的形式. 如果所化的形式为引理中第二种形式，那么右下角的子矩阵可进一步通过相应的带余除式作行变换. 如此进行下去，直到右下角的子矩阵化为引理 2.5.2 中第一种形式.

令

$$w_\ell = \sum_{i=0}^{\ell} \delta_i = \deg f_0 - \deg f_{\ell+1},\ \ell = 0, \cdots, s-1.$$

设 $w_{\ell-1} < k \leqslant w_\ell$, $0 \leqslant \ell \leqslant s-1$. 由上面的讨论知，经过 $\sum\limits_{i=0}^{\ell-1} \frac{1}{2}\delta_i(\delta_i - 1) + \frac{1}{2}(k - w_{\ell-1})(k - w_{\ell-1} - 1) + 2m$ 次第一类初等行变换和若干次第二类初等行变换，其中 $m \in \mathbb{N}$, 矩阵 $S(f,g;k)$ 可化为如下形式的上三角矩阵：

$$\Delta := \left(\begin{array}{c}
T(f_0; \delta_0, k - w_0) \\ \hline
\begin{array}{c|c} O & T(f_1; \delta_0 + \delta_1, k - w_1) \end{array} \\ \hline
\cdots\cdots \\ \hline
\begin{array}{c|c} O & T(f_{\ell-1}; \delta_{\ell-2} + \delta_{\ell-1}, k - w_{\ell-1}) \end{array} \\ \hline
\begin{array}{c|c} O & T(f_\ell; k - w_{\ell-1} + \delta_{\ell-1}, 0) \end{array} \\ \hline
\begin{array}{c|c} O & T(f_{\ell+1}; k - w_{\ell-1}, 0) \end{array}
\end{array}\right).$$

由行列式的性质知，在 $S(f,g;k)$ 和 Δ 中，位置相同的 $2k$ 级子式仅相差同一符号.

当 $k < w_\ell$ 时，在上面矩阵 Δ 的最后一行中左端零元的个数为： $\deg f_0 + k - \deg f_{\ell+1} - 1 = k + w_\ell - 1 \geqslant 2k$. 因而， Δ 的左端 $2k$ 级子式为零. 从而 $S(f,g;k)$ 的左端 $2k$ 级子式为零，即 $D_{2k} = 0$.

当 $k = w_\ell$ 即 $k - w_{\ell-1} = \delta_\ell$ 时， Δ 的左端 $2k$ 级子式为上三角行列式，其值为

$$\begin{aligned}
d_{2k} := {} & c_0^{\delta_0} c_1^{\delta_0+\delta_1} \cdots c_\ell^{\delta_{\ell-1}+\delta_\ell} c_{\ell+1}^{\delta_\ell} \\
= {} & (c_0 c_1)^{\delta_0} (c_1 c_2)^{\delta_1} \cdots (c_\ell c_{\ell+1})^{\delta_\ell}.
\end{aligned}$$

由行列式的性质即有

$$D_{2k} = (-1)^{\sum_{i=0}^{\ell} \frac{1}{2}\delta_i(\delta_i - 1) + 2m} d_{2k} = (-1)^{e_k} d_{2k}.$$

注意到 $\deg f_{\ell+1} = \deg f_0 - k = n - k$, 从而令 $f_{\ell+1}(x) = c_{\ell+1}x^{n-k} + b_1x^{n-k-1} + \cdots + b_{n-k}$. 此时易见, Δ 中前 $2k-1$ 列和第 $2k+t$ $(1 \leqslant t \leqslant n-k)$ 列所构成的 $2k$ 级子式 $d_{(2k,t)}$ 与左端 $2k$ 级子式 d_{2k} 相比较, 除左下角元素分别为 b_t 和 $c_{\ell+1}$ 外, 主对角线上其他元素都相同. 从而有 $b_t = c_{\ell+1}\dfrac{d_{(2k,t)}}{d_{2k}} = c_{\ell+1}\dfrac{D_{(2k,t)}}{D_{2k}}$, $t = 1, \cdots, n-k$. 于是有

$$f_{\ell+1}(x) = c_{\ell+1}\sum_{t=0}^{n-k}\frac{D_{(2k,t)}}{D_{2k}}x^{n-k-t}.$$

只剩下考虑 $k > w_{s-1}$ 的情形. 当 $k > w_{s-1}$ 时, 对矩阵 $S(f,g;k)$ 作一系列如上初等行变换. 此时易知, 最后所化成的矩阵至少有一行元素全为零. 从而 $D_{2k} = 0$. 证毕.

现在, 我们来建立本节中主要结论 —— 定理 2.5.4. 在此之前, 我们还需要引进一个概念.

对于域 F 中元素序列 $a_1, \cdots, a_n$, 其中 $a_1 \neq 0$, 可得到它的符号表:

$$e_1 = \text{sgn}(a_1), \cdots, e_n = \text{sgn}(a_n),$$

其中 $\text{sgn}(a_i)$ 为元素 a_i 关于正锥 P 的符号, $i = 1, \cdots, n$.

只要在上面符号表中有零介于两个非零元之间, 我们将对上面符号表进行这样的修订: 对于表中每个如下符号段

$$[e_i, 0, \cdots, 0, e_{i+\delta}],$$

其中 $e_ie_{i+\delta} \neq 0$ 且 $\delta > 0$, 代之以如下项数相同的符号段

$$[e_i, -e_i, -e_i, e_i, e_i, -e_i, \cdots, (-1)^{\frac{\delta(\delta-1)}{2}}e_i, e_{i+\delta}].$$

容易看出, 对于如上原来的符号段, 修订后的符号段中变号数等于

$$\begin{aligned}&\sum_{j=1}^{\delta-1}\frac{1-(-1)^j}{2} + \frac{1-(-1)^{\frac{\delta(\delta-1)}{2}}\text{sgn}(e_ie_{i+\delta})}{2}\\ &= \frac{1}{2}\Big(\delta + \frac{1+(-1)^\delta}{2} - (-1)^{\frac{\delta(\delta-1)}{2}}\text{sgn}\big(\frac{a_{i+\delta}}{a_i}\big)\Big).\end{aligned}$$

对修订后的各个符号段中变号数求和, 即可计算出整个修订符号表的变号数, 这一变号数称作原序列 $a_1, \cdots, a_n$ 的修订变号数.

定理 2.5.4 设 $f(x)$ 是域 F 上的一个 n 次多项式, $D_2, \cdots, D_{2n}$ 是矩阵 Sylvester(f) 的偶次顺序主子式, D_{2r} 是其中最后一个非零者, 且记 v 为序列 $D_2, \cdots, D_{2n}$ 的修订变号数, 则

(1) $f(x)$ 在 $R(\sqrt{-1})$ 中相异共轭虚根对的数目等于 v.

(2) $f(x)$ 在 R 中相异根的数目为 $r-2v$.

(3) α 是 $f(x)$ 的 m 重根, 当且仅当 α 是如下多项式的 $m-1$ 重根:

$$g(x)=\sum_{t=0}^{n-r}\frac{D_{(2k,t)}}{D_{2k}}x^{n-m-t}.$$

证明 设 $f(x)$ 和微商 $f'(x)$ 的 Sturm 序列为

$$f_0=f(x),\ f_1=f'(x),\ f_2,\ \cdots,\ f_s,$$

其中 f_s 为 $f(x)$ 和 $f'(x)$ 的一个最大公因式.

记 $d_i=\deg f_i$, $i=0,1,\cdots,s$. 再令 $\delta_j=d_j-d_{j+1}$, $j=0,1,\cdots,s-1$, 且令 $w_\ell=\sum_{j=0}^{\ell}\delta_j=d_0-d_{\ell+1}$, $\ell=0,1,\cdots,s-1$. 根据定理 2.5.3, 矩阵 Sylvester(f) 的偶次顺序主子式中的非零者依次为

$$D_2=D_{2w_0},\ D_{2w_1},\ \cdots,\ D_{2w_{s-1}}.$$

由条件知, $r=w_{s-1}=d_0-d_s=\deg(\frac{f_0}{f_s})$. 由于多项式 $\frac{f_0}{f_s}$ 在 $R(\sqrt{-1})$ 中的根恰好为 $f(x)$ 在 $R(\sqrt{-1})$ 中的全部相异根. 从而可知, $f(x)$ 在 $R(\sqrt{-1})$ 中的相异根个数为 r.

又令 c_i 为 f_i 的首项系数, $i=0,1,\cdots,s$. 由定理 2.4.6 的推论 2 知, $f(x)$ 在 R 中的相异根个数为序列 $\{(-1)^{d_0}c_0,(-1)^{d_1}c_1,\cdots,(-1)^{d_s}c_s\}$ 和序列 $\{c_0,c_1,\cdots,c_s\}$ 的变号数之差, 即等于

$$\begin{aligned}&\sum_{i=0}^{s-1}\frac{1-(-1)^{d_i+d_{i+1}}\mathrm{sgn}(c_ic_{i+1})}{2}-\sum_{i=0}^{s-1}\frac{1-\mathrm{sgn}(c_ic_{i+1})}{2}\\ =&\sum_{i=0}^{s-1}\frac{\mathrm{sgn}(c_ic_{i+1})-(-1)^{\delta_i}\mathrm{sgn}(c_ic_{i+1})}{2}\\ =&\sum_{\substack{0\leqslant i\leqslant s-1\\ 2|\delta_i+1}}\mathrm{sgn}(c_ic_{i+1}).\end{aligned}$$

注意到, 在序列 $D_2, \cdots, D_{2n}$ 中, 需要修订的元素段为

$$[D_{2w_{i-1}},0,\cdots,0,D_{2w_i}],\quad i=1,\cdots,s-1.$$

根据定理 2.5.3 和修订变号数的分段计算法，我们有

$$\begin{aligned} r-2v = &\ r-\sum_{i=1}^{s-1}\left(\delta_i+\frac{1+(-1)^{\delta_i}}{2}-(-1)^{\frac{\delta_i(\delta_i-1)}{2}}\mathrm{sgn}(\frac{D_{2w_i}}{D_{2w_{i-1}}})\right)\\ = &\ \delta_0+\sum_{i=1}^{s-1}((-1)^{\frac{\delta_i(\delta_i-1)}{2}}\mathrm{sgn}(\frac{D_{2w_i}}{D_{2w_{i-1}}})-\frac{1+(-1)^{\delta_i}}{2})\\ = &\ 1+\sum_{i=1}^{s-1}(\mathrm{sgn}(c_ic_{i+1})^{\delta_i}-\frac{1+(-1)^{\delta_i}}{2})\\ = &\ \mathrm{sgn}(c_0c_1)+\sum_{\substack{1\leqslant j\leqslant s-1\\ 2\mid\delta_i+1}}\mathrm{sgn}(c_ic_{i+1})=\sum_{\substack{0\leqslant j\leqslant s-1\\ 2\mid\delta_i+1}}\mathrm{sgn}(c_ic_{i+1}). \end{aligned}$$

再由定理 2.5.3 可知， $f_s(x)=c_sg(x)$. 从而 $g(x)$ 也是 $f(x)$ 和 $f'(x)$ 的一个最大公因式. 根据关于根的重数的熟知事实，定理中结论 (3) 成立. 至此定理获证.

上面定理是由杨路等人提出的. 对于一个具有参数的多项式，可通过定理 2.5.4 获得一些仅含参数的多项式关系式组，这些关系式组构成一个判定所给多项式的实根与虚根的个数和重数的完备系统. 因而，这些关系式组被称作所给多项式的判别系统. 在文献 [198] 中，一个关于六次一般多项式的判别系统被建立.

§2.6 序域的单超越扩张

在 §2.3 中，我们建立了关于序 (正锥) 在单代数扩张上拓展的一个结论，见定理 2.3.8 在这一节中，我们将对序域的单超越扩张进行讨论.

设 $(F,\leqslant)$ 是一个序域， t 是 F 上的一个超越元. 为研究 $\leqslant$ 在 $F(t)$ 上的拓展，可先将序域 $(F,\leqslant)$ 扩充为它的实闭包 R, 然后再讨论 R 的惟一序在 $R(t)$ 上的拓展，最后将拓展的序限制到子域 $F(t)$, 即得 $\leqslant$ 在 $F(t)$ 上的拓展. 实际上，域 F 的序 $\leqslant$ 在 $F(t)$ 上的所有拓展与 $R(t)$ 的所有序之间存在一个一一对应.

命题 2.6.1 设 (F,P) 是一个序域， t 是 F 上一个超越元， R 为 (F,P) 的实闭包，记 $\mathcal{X}_{R(t)}$ 为 $R(t)$ 的所有正锥组成的集合，且 $\mathcal{X}_{F(t)}(P)$ 为正锥 P 在 $F(t)$ 上的所有拓展组成的集合，则 $\mathcal{X}_{R(t)}$ 到 $\mathcal{X}_{F(t)}(P)$ 的如下限制映射:

$$r:\quad Q\mapsto Q\cap F(t),\qquad Q\in\mathcal{X}_{R(t)},$$

是一个一一对应.

证明 设 $P_1\in\mathcal{X}_{F(t)}(P)$. 令 R_1 是 $(F(t),P_1)$ 的实闭包，且 R_0 是 F 在 R_1 中的代数闭包. 由命题 2.1.5 可知， R_0 也是 (F,P) 的实闭包. 根据实闭包的惟一性，存在 R 到 R_0 的一个 F- 同构 τ. 注意到 t 是 R 和 R_0 上的超越元. 从而 τ 可拓展成 $R(t)$ 到 R_1 的一个嵌入 π ，使得 $\pi(t)=t$. 令 $Q=\pi^{-1}(R_1^2)$, 则易知， Q 是 $R(t)$ 的一个正锥，使得 $Q\cap F(t)=P_1$. 因而，映射 r 是一个满射.

又设 $Q_1, Q_2 \in \mathcal{X}_{R(t)}$, 且 $Q_1 \cap F(t) = Q_2 \cap F(t)$. 令 R_1 和 R_2 分别是 $(R(t), Q_1)$ 和 $(R(t), Q_2)$ 的实闭包. 显然, R_1 和 R_2 都是序域 $(F(t), P_1)$ 的实闭包, 这里 $P_1 := Q_1 \cap F(t) = Q_2 \cap F(t)$. 根据实闭包的惟一性, 存在 R_1 到 R_2 的一个 $F(t)-$ 同构 π. 由于 R 是 F 在 R_1 中的代数闭包, 从而 $\pi(R)$ 是 F 在 R_2 中的代数闭包. 注意到 R 是 F 在 R_2 中的代数闭包, 从而 $\pi(R) = R$. 这表明 π 在 R 上的限制 $\pi\mid_R$ 是 R 的一个 $F-$ 自同构. 由定理 2.3.7 的推论知, $\pi\mid_R$ 是 R 的恒等自同构. 由此可知, π 在 $R(t)$ 上的限制 $\pi\mid_{R(t)}$ 是 $R(t)$ 的一个恒等自同构. 于是 $Q_1 = \pi(Q_1) = \pi(R_1^2 \cap R(t)) \subseteq \pi(R_1^2) \cap \pi(R(t)) = R_2^2 \cap R(t) = Q_2$, 从而必有 $Q_1 = Q_2$. 因而, 映射 r 是一个单射. 证毕.

鉴于上面的命题, 本节的讨论将从考察实闭域的单超越扩张上的序而展开.

定义 2.6.1 设 (F, P) 是一个序域. F 的一个子集 D 称作 F 关于 P (或序 $\leqslant_P$) 的一个分割, 如果对于每个 $a \in F$, 只要有某个 $d \in D$, 使得 $a \leqslant_P d$, 总有 $a \in D$.

当 R 是一个实闭域时, R 关于它的惟一正锥 (序) 的分割简称 R 的一个分割. 为方便起见, 对于实闭域 R 的一个分割 D, 下列记号将采用: 当 $D = \phi$ 时, 记 $D = D_{-\infty}$; 当 $D = R$ 时, 记 $D = D_{+\infty}$; 当 D 中有最大元素 b 时, 记 $D = D_{b+}$; 而当 $R \setminus D$ 中有最小元素 b 时, 记 $D = D_{b-}$. 注意, 除这四种类型的分割外, 还有另外的分割. 除上面所列的四种分割外的其他分割称作超越分割.

例 1 设 R 是有理数域 $\mathbb{Q}$ 在实数域 $\mathbb{R}$ 中的代数闭包. 由命题 2.1.5 知, R 是一个实闭域. 令 $\pi = 3.1415\cdots$ 是熟知的圆周率, 则 $\pi \in \mathbb{R}$, 但 $\pi \notin R$. 作 R 的如下集合:

$$D = \{a \in R \mid a < \pi\}.$$

易见, D 是 R 的一个分割, 且 D 是一个超越分割.

命题 2.6.2 设 R 同上, t 是 R 上一个超越元, 则 $R(t)$ 的全部序与 R 的全部分割之间存在一个一一对应.

证明 对于任意 $Q \in \mathcal{X}_{R(t)}$, 可构造 R 的如下子集:

$$D(Q) := \{a \in R \mid a \leqslant_Q t\},$$

这里, $\leqslant_Q$ 是 Q 的对应序. 易证, $D(Q)$ 是 R 的一个分割.

从而, 有一个从 $R(t)$ 的全体序 $\mathcal{X}_{R(t)}$ 到 R 的全体分割 $\mathcal{D}_R$ 的如下映射:

$$\phi: \quad Q \longmapsto D(Q), \quad Q \in \mathcal{X}_{R(t)}.$$

对于 $D \in \mathcal{D}_R$, 令 Q^D 是乘法群 $\dot{R}(t)$ 中由全部如下四种元素所生成的子群:

(1) a^2, 其中 a 取遍 R 中全部非零元素, 即 $a \in \dot{R}$;

(2) $t - d$, 其中 $d \in D$;

(3) $e-t$, 其中 $e\in R\setminus D$;

(4) $(t+b)^2+c^2$, 其中 $b,c\in R$ 且 $c\neq 0$.

对于每个非零多项式 $f(t)\in R[t]$, 由定理 2.1.3 知, $f(t)$ 可表示为

$$f(t)=a\left[\sum_{i=1}^{n}(t-d_i)\right]\left[\sum_{j=1}^{m}(e_j-t)\right]\left\{\sum_{k=1}^{s}[(t+b_k)^2+c_k^2]\right\},$$

其中 n, m 和 s 均为非负整数, $d_i\in D$, $e_j\in R\setminus D$, a, b_k, $c_k\in R$, 且 a 和 c_k 不为零, $i=1,\cdots,n$; $j=1,\cdots,m$; $k=1,\cdots,s$.

根据 $a\in R^2$ 或 $a\in -R^2$, 分别有 $f(x)\in Q^D$ 或 $f(x)\in -Q^D$. 由此有, $\left(\dfrac{f(t)}{g(t)}\right)^2\in Q^D$, 对于任意非零 $f(t),g(t)\in R[t]$.

此外, 可断言: 对于两个多项式 $f(t),g(t)\in Q^D$, $f(t)+g(t)\in Q^D$. 事实上, 如若不然, 则 $f(t)+g(t)=0$ 或 $f(t)+g(t)\in -Q^D$, 即 $f(t)+g(t)=-h(t)$, 对于某个 $h(t)\in Q^D$. 由 Q^D 的定义, $f(t),g(t)$ 和 $h(t)$ 均可表示为有限个如上四种元素以及它们的逆的乘积. 从而这些元素只涉及有限个如下两种形式的一次因式: (1)$t-d_i$, 其中 $d_i\in D$, $i=1,\cdots,r$; (2)e_j-t, 其中 $e_j\in R\setminus D$, $j=1,\cdots,s$. 此时, 必有 $b\in R$, 使得 $d_i<b<r_j$, $i=1,\cdots,r$; $j=1,\cdots,s$. 将 $t=b$ 代入 $f(t),g(t)$ 与 $h(t)$, 则 $f(b)$, $g(b)$ 与 $h(b)$ 均为 R 中正元素. 然而, $f(b)+g(b)=0$ 或 $f(b)+g(b)=-h(b)$, 矛盾. 由此断言易知, Q^D 对于加法也是封闭的.

现令 $Q_D=Q^D\cup\{0\}$. 由上面的讨论知, Q_D 对于 $R(t)$ 的乘法与加法都是封闭的. 此外, $-1\notin Q_D$; 否则有 $-1,1\in Q^D$, 进而 $0=(-1)+1\in Q^D$. 对于任意 $\dfrac{f(t)}{g(t)}\in R(t)$, 其中 $f(t),g(t)$ 均为 $R[t]$ 中非零多项式. 由上面讨论知, $g^2(t)\in Q^D$, $f(t)g(t)\in Q^D$ 或 $-Q^D$. 从而 $\dfrac{f(t)}{g(t)}\in Q^D\subseteq Q_D$, 或 $\dfrac{f(t)}{g(t)}\in -Q^D\subseteq -Q_D$. 因而, $R(t)=Q_D\cup -Q_D$. 根据定义 1.1.2, $Q_D\in\mathcal{X}_{R(t)}$, 即 Q_D 是 $R(t)$ 的一个序.

这样, 我们可规定 $\mathcal{D}_R$ 到 $\mathcal{X}_{R(t)}$ 的如下映射:

$$\psi:\quad D\longmapsto Q_D,\quad D\in\mathcal{D}_R.$$

进一步可验证, ψ 是 ϕ 的逆映射. 因此, ϕ 是一个一一对应. 证毕.

由上面命题, 容易建立下面的定理 2.6.3.

定理 2.6.3 设 R 是一个实闭域, 且 t 是 R 上一个超越元, 则 $R(t)$ 的每个序（正锥）恰好是如下形式之一:

(1) $Q_{+\infty}:=\{\dfrac{f}{g}\mid f,g\in R[t],\ f=0$ 或 fg 的首项系数为正 $\}$;

(2) $Q_{-\infty}:=\{\dfrac{f}{g}\mid f,g\in R[t],\ f=0$ 或 $f(-t)g(-t)$ 的首项系数为正 $\}$;

(3) $Q_{a+} := \{\frac{f}{g} \mid f,\, g \in R[t],\, f = 0$ 或 $f(t+a)g(t+a)$ 的尾项系数为正 $\}$, 对于某个 $a \in R$;

(4) $Q_{a-} := \{\frac{f}{g} \mid f,\, g \in R[t],\, f = 0$ 或 $f(a-t)g(a-t)$ 的尾项系数为正 $\}$, 对于某个 $a \in R$;

(5) $Q_D = \{\frac{f}{g} \mid f,\, g \in R[t],\, f = 0$ 或有某个 $d \in D$ 以及 $e \in R \setminus D$, 使得 $f(t)g(t)$ 在区间 $]d, e[$ 上取正值 $\}$, 对于 R 的某个超越分割 D.

此外, $R(t)$ 的一个序 Q 是在 R 上的阿基米德序, 当且仅当对于 R 的某个超越分割 D, $Q = Q_D$.

证明 设 Q 是 $R(t)$ 的一个任意序, 则命题 2.6.1 知, $Q = Q_D$, 这里 D 是 R 的某个分割. 根据分割的分类, 我们有如下可能情形:

(1) $D = D_{+\infty} = R$. 根据命题 2.6.1 的证明中关于 Q_D 的规定可知, $Q_D \subseteq Q_{+\infty}$. 再根据 §1.1 中例 3, $Q_{+\infty}$ 是 $R(t)$ 的一个序. 从而必有 $Q_D = Q_{+\infty}$, 即 $Q = Q_{+\infty}$.

(2) $D = D_{-\infty} = \phi$. 通过类似于情况 (1) 的讨论可知, $Q = Q_{-\infty}$.

(3) $D = D_{a+}$, 其中 a 是 D 中最大元素. 由 Q_D 的规定可知, $Q_D \subseteq Q_{a+}$. 再根据定义 1.1.2 可验证, Q_{a+} 是 $R(t)$ 的一个序. 从而必有 $Q_D = Q_{a+}$, 即 $Q = Q_{a+}$.

(4) $D = D_{a-}$, 其中 a 是 $R \setminus D$ 中最小元素. 类似地可证, $Q = Q_{a-}$.

(5) D 是一个超越分割. 记 $Q' = \{\frac{f}{g} \mid f,\, g \in R[t],\, f = 0$ 或有某个 $d \in D$ 以及 $e \in R \setminus D$, 使得 $f(t)g(t)$ 在区间 $]d, e[$ 上取正值 $\}$. 对于非零的 $\frac{f(t)}{g(t)} \in Q_D$, 其中 $f(t),\, g(t) \in R[t]$, $f(t)g(t) \in Q^D$. 由 Q^D 的规定可知, $f(t)g(t)$ 可表为如下形式:

$$f(t)g(t) = a^2 \left[\sum_{i=1}^{n}(t-d_i)\right] \left[\sum_{j=1}^{m}(e_j - t)\right] \left\{\sum_{k=1}^{s}[(t+b_k)^2 + c_k^2]\right\},$$

其中 n, m 和 s 均为非负整数, $d_i \in D$, $e_j \in R \setminus D$, a, b_k, $c_k \in R$ 且 a 和 c_k 不为零, $i = 1, \cdots, n$; $j = 1, \cdots, m$; $k = 1, \cdots, s$.

若 $n \geqslant 1$, 令 $d = \max\{d_i \mid i = 1, \cdots, n\}$; 否则令 d 为 D 中任一元素. 此外, 令 $e = \min\{e_j \mid j = 1, \cdots, m\}$, 若 $m \geqslant 1$; 否则令 e 为 $R \setminus D$ 中任一元素. 由于 D 是一个超越分割, 从而必有 $d < e$. 此时显见, $f(t)g(t)$ 在 $]d, e[$ 上取正值. 从而 $\frac{f(t)}{g(t)} \in Q'$, 即有 $Q_D \subseteq Q'$. 根据定义 1.1.2 易知, Q' 是 $R(t)$ 的一个序. 因而, $Q = Q_D = Q'$.

注意到, 在情况 (1) 和 (2) 中, t 是在 R 上的 (正或负) 无限大元素; 而在情况 (3) 和 (4) 中, $t - a$ 是在 R 上的 (正或负) 无限小元素. 因而, 这四种情况下的序都是在 R 上的非阿基米德序. 现设 $Q = Q_D$, 其中 D 是 R 的一个超越

分割，且 $\frac{f(t)}{g(t)} \in Q_D$，其中 $f(t)$, $g(t)$ 均为 $R[t]$ 中非零多项式．显然， $f(t)g(t)$, $g^2(t) \in Q_D$．由上面的论证知，有 $d \in D$ 以及 $e \in R \setminus D$, 使得 $f(t)g(t)$ 和 $g^2(t)$ 在 $]d,e[$ 上都取正值．由适合实闭域的最值定理，在闭区间 $[d,e]$ 上 $f(t)g(t)$ 有最大值 M, 而 $g^2(t)$ 有最小值 m．显然， $M>0$ 且 $m>0$．此时易知，在 $]d,e[$ 上，$m(M-f(t)g(t))+M(2g^2(t)-m)$ 取正值，即有 $m(M-f(t)g(t))+M(2g^2(t)-m) \in Q$．从而 $\frac{2M}{m}-\frac{f(x)}{g(x)}=\frac{m(M-f(t)g(t))+M(2g^2(t)-m)}{mg^2(t)} \in Q$，即 $\frac{f(t)}{g(t)} <_Q \frac{2M}{m}$．这表明， Q 是在 R 上的一个阿基米德序．至此，定理获证．

现在，我们可以建立下面定理．

定理 2.6.4　设 (F,P) 是一个实闭包为 R 的序域， t 是 F 上的一个超越元，则正锥 P 在 $F(t)$ 上的每个拓展恰好是如下形式之一：

(1) $Q_{+\infty} \cap F(t)$;

(2) $Q_{-\infty} \cap F(t)$;

(3) $Q_{a+} \cap F(t)$, 对于某个 $a \in R$;

(4) $Q_{a-} \cap F(t)$, 对于某个 $a \in R$;

(5) $Q_D \cap F(t)$, 对于 R 的某个超越分割 D.

其中符号 $Q_{+\infty}, Q_{-\infty}, Q_{a+}, Q_{a-}$ 和 Q_D 的意义同定理 2.6.3．此外， P 在 $F(t)$ 上的拓展是在 F 上的阿基米德正锥，当且仅当所拓展的正锥为 $Q_D \cap F(t)$, 这里 D 是 R 的一个超越分割．

证明　显然，上面五种形式的正锥都是 P 在 $F(t)$ 上的拓展．反过来，设 P_1 是 P 在 $F(t)$ 上的任意一个拓展．根据命题 2.6.1 知， $P_1=Q\cap F(t)$, 其中 Q 是 $R(t)$ 的一个序．再由定理 2.6.3 知， P_1 具有上面定理所示的形式．

进一步设 $P_1=Q\cap F(t)$ 是在 F 上的阿基米德序，其中 Q 是 $R(t)$ 的一个序．由定理 1.4.2 知， Q 也是在 F 上的阿基米德序，自然是在 R 上的阿基米德序．由定理 2.6.3 知， $Q=Q_D$, 其中 D 是 R 的一个超越分割．由此有 $P_1=Q_D\cap F(t)$, 其中 D 是 R 的一个超越分割．反之，若 $P_1=Q_D\cap F(t)$, 其中 D 是 R 的一个超越分割，则由定理 2.6.3 可知， P_1 是在 F 上的阿基米德序．定理获证．

定理 2.6.5　设 (F,P) 是一个序域， t 是 F 上的一个超越元，则下列叙述等价：

(1) P 在 $F(t)$ 上有一个拓展 Q, 使得 Q 在 F 上是阿基米德的；

(2) 不存在 (F,P) 到实数域 $\mathbb{R}$ 的这样一个保序嵌入 π, 使得 $\mathbb{R}$ 是 $\pi(F)$ 的代数扩张．

证明　(1) $\Longrightarrow$ (2): 设 P 在 $F(t)$ 上有一个拓展 Q, 使得 Q 在 F 上是阿基米德的．假若存在 (F,P) 到实数域 $\mathbb{R}$ 的这样一个保序嵌入 π, 使得 $\mathbb{R}$ 是 $\pi(F)$ 的代数扩张，则 (F,P) 显然是一个阿基米德序域．此时易知， $(F(t),Q)$ 也是一个阿基米德

序域. 根据定理 1.4.5, 存在 $(F(t),Q)$ 到实数域 $\mathbb{R}$ 的一个保序嵌入 τ. 注意到 τ 在 F 上的限制 $\tau|_F$ 是 (F,P) 到实数域 $\mathbb{R}$ 的一个保序嵌入. 由定理 1.4.5 中的惟一性知, $\tau|_F=\pi$. 由于 $\tau(F(t))$ 不是 $\tau(F)$ $(=\pi(F))$ 的代数扩张, 且 $\tau(F(t))\subseteq\mathbb{R}$, 从而 $\mathbb{R}$ 不是 $\pi(F)$ 的代数扩张, 矛盾. 因此, 叙述 (2) 成立.

(2) $\Longrightarrow$ (1): 设 R 为序域 (F,P) 的实闭包. 现在分情况讨论.

情况 1 (F,P) 是一个阿基米德序域. 由定理 1.4.2 知, (R,R^2) 也是一个阿基米德序域. 根据定理 1.4.5, 存在 (R,R^2) 到实数域 $\mathbb{R}$ 的一个保序嵌入 π. 由叙述 (2) 知, $\mathbb{R}$ 不是 $\pi(R)$ 的代数扩张. 从而有 $\alpha\in\mathbb{R}$, 使得 α 在 $\pi(R)$ 上是超越元. 由此可构造 R 的如下子集:

$$D_1:=\{a\in R\mid \pi(a)<\alpha\}.$$

易知, D_1 是 R 的一个超越分割.

情况 2 (F,P) 不是一个阿基米德序域. 此时有 $e\in F$, 使得 e 在有理数子域 $\mathbb{Q}$ 上是无限小元素. 由于 $-e$ 也是在有理数子域 $\mathbb{Q}$ 上的无限小元素, 从而可设 $e\in P\subseteq R^2$. 记 $e^{\frac{n-1}{n}}$ 是多项式 x^n-e^{n-1} 在 R 中惟一正根, 其中 n 为自然数. 显然, $1>_{R^2}e^{\frac{1}{2}}>_{R^2}e^{\frac{2}{3}}>_{R^2}\cdots>_{R^2}e^{\frac{n-1}{n}}>_{R^2}\cdots$. 由此可构造 R 的如下子集:

$$D_2:=\{a\in R\mid \text{对于每个自然数 } n,\ a<_{R^2}e^{\frac{n-1}{n}}\}.$$

易知, D_2 是 R 的一个分割. 注意到, $e\in D_2$, 但 $1\notin D_2$. 从而 $D_2\neq D_{+\infty}$, 且 $D_2\neq D_{-\infty}$. 设 $a\in D_2$, 其中 $0<_{R^2}e\leqslant_{R^2}a$, 则对于每个自然数 n, 都有 $a<_{R^2}e^{\frac{n}{n+1}}$. 从而 $ae^{-\frac{n-1}{n}}<_{R^2}e^{\frac{1}{n(n+1)}}$. 由于 $e^{\frac{1}{n(n+1)}}$ 在 $\mathbb{Q}$ 上是无限小, 从而 $e^{\frac{1}{n(n+1)}}<_{R^2}\dfrac{1}{2}$, 即有 $ae^{-\frac{n-1}{n}}<_{R^2}\frac{1}{2}$. 由此有 $2a<e^{\frac{n-1}{n}}$, 即 $2a\in D_2$. 显然 $a<_{R^2}2a$. 这表明: D_2 中没有最大元. 又设 $a\in R\setminus D_2$, 则对于某个自然数 k, $e^{\frac{k-1}{k}}\leqslant_{R^2}a$. 此时, $e^{\frac{k}{k+1}}\in R\setminus D_2$, 且 $e^{\frac{k}{k+1}}<_{R^2}a$. 这又表明: D_2 中没有最小元. 因而, D_2 是 R 的一个超越分割.

根据定理 2.6.4, 正锥 P 在 $F(t)$ 上有一个拓展 Q, 使得 Q 在 F 上是阿基米德的. 证毕.

第三章　实赋值与实位

在域论这一领域中, 关于赋值的研究是一个重要课题. 在本章将研究一类与实域和序域密切相关的赋值及其相应的位, 这就是所谓的实赋值和实位. 在本章中, 我们将考察实赋值 (位) 与序之间的 "相容" 关系, 实赋值 (位) 的构造与拓展, 同时建立与实赋值 (实位) 相关的重要结论. 对于赋值论的一般知识, 读者可以查阅参考书 [50] 和 [76].

§3.1　实　赋　值

为清楚起见, 在给出实赋值的定义之前, 先回顾赋值论中有关概念和基本事实.

设 G 是一个 Abel 群, 其运算记作加法: $+$. 若 G 上有一个全序 $\leqslant$, 使得对于 $a, b, c \in G$, 有 $a+c \leqslant b+c$, 只要 $a \leqslant b$, 则 $\leqslant$ 称作群 G 的一个序, 且称 $(G, \leqslant)$ 是一个序群. 在 G 上添加一个独立元素 ∞, 可得到集合 G_∞. 进一步补充规定如下: (1) 对于每个 $\alpha \in G_\infty$, $\alpha + \infty = \infty + \alpha = \infty$; (2) 对于每个 $a \in G$, $a < \infty$. 则 G_∞ 对于运算 $+$ 是一个交换半群, 且 G 的序 $\leqslant$ 被拓展到 G_∞ 上. 域 F 到 G_∞ 的一个映射 v 称作 F 的赋值, 如果下列条件成立: (1)$v(a) = \infty$ 当且仅当 $a = 0$; (2)$v(ab) = v(a) + v(b)$; (3)$v(a+b) \geqslant \min\{v(a), v(b)\}$. 此时, $v(\dot{F})$ 是 G 的一个子群, 且被称作赋值 v 的值群. 由上面条件可推出: (4)$v(1) = 0$, $v(-a) = v(a)$; (5) 若 $v(a) \neq v(b)$, 则 $v(a+b) = \min\{v(a), v(b)\}$.

域 F 的一个 (包含单位元 1 的) 子环 A 被称作 F 的一个赋值环, 若对于每个非零 $a \in F$, $a \in A$ 或 $a^{-1} \in A$. 赋值环 A 是一个局部环. 于是, A 中全部不可逆元素组成 A 的惟一极大理想 M, 且 M 被称作 A 的赋值理想. 从而, $A = M \cup U$, 且 $M \cap U = \phi$, 这里 U 是 A 中所有可逆元对于乘法组成的群. 此时, 剩余域 A/M 称作 A 的剩余域.

对于域 F 的一个赋值 v, 可定义 F 的如下子集:

$$A_v = \{a \in F \mid v(a) \geqslant 0\};$$

$$M_v = \{a \in F \mid v(a) > 0\};$$

$$U_v = \{a \in F \mid v(a) = 0\}.$$

容易验证, A_v 是 F 的一个极大理想为 M_v, 可逆元群为 U_v 的赋值环. 因而, A_v, M_v 和 U_v 分别称作 v 的赋值环, 赋值理想和可逆元群. 此外, A_v/M_v 称作赋值 v 的剩余域, 且记作 F_v.

在等价的意义下，域 F 的赋值是由它们的赋值环惟一决定的. 此外，域 F 的赋值和赋值环二者之间是可相互转化的. 对于这种转化，域的全体赋值环与所有的赋值等价类之间存在一一对应关系.

在赋值论中，下列关于单超越扩张的赋值的结论是熟知的.

命题 3.1.1 设 v 是域 $F(t)$ 的一个非浅显赋值，其中 t 是域 F 上的超越元，Γ 是 v 的值群，且对于每个非零 $a \in F$, $v(a) = 0$, 那么 Γ 序同构于加法群 $\mathbb{Z}$, 且若将 Γ 和 $\mathbb{Z}$ 等同，则有下列两种可能情况:

(1) 对于某个不可约多项式 $p(t) \in F[t]$, $v(p(t)) = 1$, 而对于 $F[t]$ 中不被 $p(t)$ 整除的多项式 $g(t)$, $v(g(t)) = 0$. 此时，v 的赋值环 $A_v = (F[t])_{(p(t))}$ (环 $F[t]$ 关于素理想 $(p(t))$ 的局部化), 剩余域 $F_v \cong F[t]/(p(t))$.

(2) 对于非零多项式 $f(t) \in F[t]$, $v(f(t)) = -\deg f(t)$, 其中 $\deg f(t)$ 表示多项式 $f(t)$ 的次数. 此时，v 的赋值环 $A_v = \{\frac{f(t)}{g(t)} \in F(t) \mid \deg f(t) \leqslant \deg g(t)\}$, 剩余域 $F_v \cong F$.

现在，我们将讨论转到本节的主要研究对象 —— 实赋值. 首先引进实赋值的定义如下.

定义 3.1.1 域 F 的一个赋值 v 称作实赋值，若 v 的剩余域 A_v/M_v 是一个实域.

根据上面定义以及赋值和赋值环之间的转化关系，域 F 的一个赋值环 A 称作实赋值环，若剩余域 A/M 是一个实域，这里 M 是 A 的赋值理想.

例 在命题 3.1.1 中，进一步设 F 是一个实闭域. 由命题 3.1.1 知，有如下三种可能:

(1.1) $F_v \cong F[t]/(p(t))$, 其中 $p(t)$ 在 F 中有根，即 $p(t)$ 是 $F[t]$ 中一次多项式. 此时，$F[t]/(p(t)) \cong F$. 从而 v 是一个实赋值.

(1.2) $F_v \cong F[t]/(p(t))$, 其中 $p(t)$ 在 F 中无根. 此时 F_v 是 F 的一个真代数扩张，从而它不是实域. 因而，v 不是实赋值.

(2) $F_v \cong F$. 此时，v 是实赋值.

根据定义 3.1.1，容易建立下面命题.

命题 3.1.2 设 v 是域 F 的一个赋值，M 是 v 的赋值理想，则下列叙述等价:

(1) v 是 F 的一个实赋值;

(2) 对于任意有限个 $a_1, \cdots, a_n \in F$, $v(a_1^2 + \cdots + a_n^2) = \min\{v(a_i^2) \mid i = 1, \cdots, n\}$;

(3) 若 $a_1^2 + \cdots + a_n^2 \in M$, 则 $a_i \in M$, $i = 1, \cdots, n$.

证明 (1) $\Longrightarrow$ (2): 不妨设 $v(a_1^2) = \min\{v(a_i^2) \mid i = 1, \cdots, n\}$. 当 $v(a_1) = \infty$ 时，必有 $v(a_i) = \infty$, 即 $a_i = 0$, $i = 1, \cdots, n$. 此时，$v(a_1^2 + \cdots + a_n^2) = v(0) =$

$\infty = v(a_1^2) = \min\{v(a_i^2) \mid i = 1, \cdots, n\}$. 下设 $v(a_1) \neq \infty$, 即 $a_1 \neq 0$. 由于 $v(a_ia_1^{-1}) = v(a_i) - v(a_1) \geqslant 0$, 从而 $a_ia_1^{-1} \in A_v$, $i = 1, \cdots, n$. 记 $\overline{a_ia_1^{-1}} := a_ia_1^{-1} + M \in F_v$, $i = 1, \cdots, n$. 由于 F_v 是实域, 从而 $\overline{1 + (a_2a_1^{-1})^2 + \cdots + (a_na_1^{-1})^2} = 1 + \overline{a_2a_1^{-1}}^2 + \cdots + \overline{a_na_1^{-1}}^2 \neq 0$, 即有 $1 + (a_2a_1^{-1})^2 + \cdots + (a_na_1^{-1})^2 \notin M$. 于是 $v(1 + (a_2a_1^{-1})^2 + \cdots + (a_na_1^{-1})^2) = 0$, 即 $v(a_1^2 + a_2^2 + \cdots + a_n^2) = v(a_1^2)$. 从而, 叙述 (2) 获证.

(2) $\Longrightarrow$ (3): 由所设知, $v(a_1^2+\cdots+a_n^2) > 0$. 根据叙述 (2), 有 $\min\{v(a_i^2) \mid i = 1, \cdots, n\} > 0$. 显然 $v(a_i) > 0$, 即 $a_i \in M$, $i = 1, \cdots, n$.

(3) $\Longrightarrow$ (1): 假若 v 不是实赋值, 则剩余域 A_v/M 不是实域. 于是有 $a_1, \cdots, a_n \in A_v$, 使得 $1 + \bar{a}_1^2 + \cdots + \bar{a}_n^2 = 0$, 其中 $\bar{a}_i := a_i + M \in A_v/M$, $i = 1, \cdots, n$. 从而 $1 + a_1^2 + \cdots + a_n^2 \in M$. 由叙述 (3), 有 $1 \in M$, 矛盾. 因此, v 是一个实赋值. 证毕.

推论 1 设 v 是域 F 的一个非浅显赋值, A 是 v 的赋值环, 则 v 是 F 的一个实赋值, 当且仅当由关系式 $a_1^2 + \cdots + a_n^2 \in A$, 其中 $a_1, \cdots, a_n \in F$, 可推出 $a_i \in A$, $i = 1, \cdots, n$.

证明 必要性: 设 $a_1^2 + \cdots + a_n^2 \in A$, 其中 $a_i \in F$, $i = 1, \cdots, n$, 则由命题 3.1.2 知, $\min\{v(a_i^2) \mid i = 1, \cdots, n\} = v(a_1^2 + \cdots + a_n^2) \geqslant 0$. 从而 $v(a_i) \geqslant 0$, 即 $a_i \in A$, $i = 1, \cdots, n$.

充分性: 设 $a_1^2+\cdots+a_n^2 \in M$, 其中 $a_i \in F$, $i = 1, \cdots, n$. 令 $b = a_1^2+\cdots+a_n^2$, 则显然 $v(b) > 0$. 当 $b \neq 0$ 时, $(a_1^2+\cdots+a_n^2)^2b^{-2} = 1 \in A$. 注意到, $(a_1^2+\cdots+a_n^2)^2b^{-2}$ 的展开式是 F 中元素的平方和, 且其中含有 $(a_i^2b^{-1})^2$, $i = 1, \cdots, n$. 由所设知, $a_i^2b^{-1} \in A$, 即 $v(a_i^2b^{-1}) \geqslant 0$, $i = 1, \cdots, n$. 从而 $2v(a_i) = v(a_i^2) = v(a_i^2b^{-1}) + v(b) > 0$, 即有 $a_i \in M$, $i = 1, \cdots, n$. 下设 $b = 0$. 由于 v 是非浅显的, 从而 $M \neq \{0\}$, 即有非零 $a \in M$. 此时, $a^2 + a_1^2 + \cdots + a_n^2 \in M$, 且 $a^2 + a_1^2 + \cdots + a_n^2 \neq 0$. 重复上面的论证, 可得 $a_i \in M$, $i = 1, \cdots, n$. 由命题 3.1.2 知, v 是 F 的一个实赋值. 证毕.

应注意, 当 v 是浅显赋值时, 上面推论的必要性显然成立, 但充分性未必成立. 例如, 若 v 是复数域 $\mathbb{C}$ 上的浅显赋值, 则 v 显然不是实赋值, 因为剩余域 $F_v \cong \mathbb{C}$. 然而, 赋值环 $A_v = \mathbb{C}$ 满足上面推论中所提及的条件.

推论 2 若 v 是域 F 的一个实赋值, 则 F 是实域.

证明 设 M 是 v 的赋值理想. 假若 F 不是一个实域, 则有 $a_1, \cdots, a_n \in F$, 使得 $1 + a_1^2 + \cdots + a_n^2 = 0 \in M$. 由命题 3.1.2 中蕴含关系 "(1) $\Rightarrow$ (3)" 知, $1 \in M$, 矛盾! 因此, F 是一个实域. 证毕.

根据上面的推论 2, 若 v 是域 F 的一个实赋值, 则 F 是一个实域, 从而 F 有序. 自然会问: F 的某些序是否与 v 具有某种密切关系? 这种密切关系具有何种表达形式? 这些问题涉及到下面的定义.

定义 3.1.2 设 v 是域 F 的一个赋值，$\leqslant$ 是域 F 的一个序. 称 v 与序 $\leqslant$ (或称 $\leqslant$ 与 v) 相容，如果由关系式 $0 < a \leqslant b$ 可推出 $v(a) \geqslant v(b)$. 此时亦称 v 与正锥 P (或 P 与 v) 相容，这里 P 是序 $\leqslant$ 的对应正锥.

定义 3.1.3 设 $\preceq$ 是任意集合 S 的一个全序. S 的一个非空子集 C 称作是关于 $\preceq$ 的凸子集，若对于 $c_1, c_2 \in C$, 由关系式 $c_1 \preceq a \preceq c_2$ 可推出 $a \in C$.

对于域 F 的一个序 $\leqslant$ 以及任意非空子集 D, 可构造 F 的如下子集:

$$C(D, \leqslant) := \{a \in F \mid \text{存在某个 } d \in D, \text{使得 } -d \leqslant a \leqslant d\}.$$

容易验证，上面构造的子集 $C(D, \leqslant)$ 是 F 的一个关于序 $\leqslant$ 的凸子集. 这样的凸子集称作 D 关于 $\leqslant$ 的凸包. 显然，当 D 是 F 的一个子环时，$C(D, \leqslant)$ 也是 F 的一个子环. 此外，对于 F 的每个关于序 $\leqslant$ 的凸子环 C, 都有 $C(D, \leqslant) \subseteq C$, 只要 $D \subseteq C$.

命题 3.1.3 设 v 是域 F 的一个赋值，$\leqslant$ 是 F 的一个序，则下列叙述等价:

(1) v 与 $\leqslant$ 相容;

(2) A_v 关于 $\leqslant$ 是凸的;

(3) M_v 关于 $\leqslant$ 是凸的;

(4) 由关系式 $a \in M_v$ 可推出 $a < 1$, 即 $1 + M_v \subseteq P$, 这里 P 是序 $\leqslant$ 的对应正锥.

证明 (1) $\Longrightarrow$ (2): 若 $0 \leqslant a \leqslant b \in A_v$, 则由定义 3.1.2 知，$v(a) \geqslant v(b) \geqslant 0$. 从而 $a \in A_v$. 这表明，A_v 是关于 $\leqslant$ 的凸子集.

(2) $\Longrightarrow$ (3): 设 $0 < a < b \in M_v$, 则 $0 < b^{-1} < a^{-1}$. 由于 $b^{-1} \notin A_v$, 从而由叙述 (2) 知，$a^{-1} \notin A_v$, 即 $a \in M_v$. 因而，叙述 (3) 成立.

(3) $\Longrightarrow$ (4): 如若叙述 (4) 不成立，则对于某个 $a \in M$, $0 < 1 \leqslant a$. 由于 M_v 关于 $\leqslant$ 是凸的，从而 $1 \in M_v$, 矛盾. 因而，叙述 (4) 成立.

(4) $\Longrightarrow$ (1): 设 $0 < a \leqslant b$. 假若 $v(a) < v(b)$, 则 $ba^{-1} \in M_v$. 由叙述 (4) 知，$ba^{-1} < 1$, 即 $b < a$, 矛盾. 从而 $v(a) \geqslant v(b)$. 因此 v 与 $\leqslant$ 相容. 证毕.

推论 1 设 v 是域 F 的一个赋值，P 是 F 的一个正锥，则 v 与 P 相容，当且仅当 P 在剩余域 A_v/M_v 上所诱导的如下子集:

$$P_v := \{\bar{a} = a + M \mid a \in P \cap A_v\}$$

是剩余域 A_v/M_v 的一个正锥.

证明 显然，无论 v 是否与 P 相容，总有 $P_v + P_v \subseteq P_v$, $P_v \cdot P_v \subseteq P_v$ 且 $A_v/M_v = P_v \cup -P_v$.

先设 v 与 P 相容. 假若 $-1 \in P_v$, 则对于某个 $a \in P \cap A_v$, $-1 = \bar{a}$. 由此有 $-1 = a + \eta$, 对于某个 $\eta \in M_v$. 由命题 3.1.3 知，$-a = 1 + \eta \in P$. 从而 $a \in P \cap -P$,

即 $a=0$. 于是 $-1=\eta\in M_v$, 矛盾. 因而 $-1\notin P_v$. 根据定义 1.1.2 知, P_v 是 A_v/M_v 的一个正锥.

现设 P_v 是 A_v/M_v 的一个正锥. 假若 v 与 P 不相容, 则由命题 3.1.3 知, 有某个 $\eta\in M_v$, 使得 $1\leqslant_P\eta$, 即 $\eta-1\in P$. 从而 $-1=\overline{\eta-1}\in P_v$, 这是不可能的. 因此, v 与 P 相容. 证毕.

设 v 是域 F 的一个赋值, $\leqslant$ 是 F 的一个序, P 是 $\leqslant$ 的对应正锥. 当 v 与 $\leqslant$ 相容时, 由上面推论 1 知, P 在剩余域 A_v/M_v 上诱导出一个正锥 P_v. 因而, A_v/M_v 有一个正锥为 P_v 的序, 这个序将称作由 $\leqslant$ 在 A_v/M_v 上所诱导的序, 且常记作 $\leqslant_v$. 此时容易知道, 对于 A_v 中可逆元 a, $0<_v\bar{a}:=a+M_v$ 当且仅当 $0<a$.

现转换思考的角度, 考虑这样的 "提升" 问题: 设 v 是域 F 的一个赋值, 且 P_v 是剩余域 A_v/M_v 的一个正锥. 是否 F 有一个正锥 P, 使得 P_v 恰好为由 P 在 A_v/M_v 上所诱导的正锥? 回答是肯定的.

推论 2　设 v 是域 F 的一个赋值, 且 P_v 是 v 的剩余域 A_v/M_v 的一个正锥, 则 F 有一个正锥 P, 使得 v 与 P 相容, 且 P_v 恰好为由 P 在 A_v/M_v 上所诱导的正锥.

证明　考虑 F 的如下子集:

$$C:=\{a\in A_v\mid a\notin M_v,\ a+M\in P_v\}.$$

显然, $1\in C, C+C\subseteq C$, 且 $C\cdot C\subseteq C$.

在此基础上, 再构造 F 的如下子集:

$$T:=\left\{\sum_{i=1}^{n}c_ia_i^2(1-\eta_i)\mid c_i\in C,\ a_i\in F,\ \eta_i\in M_v,\ i=1,\cdots,n\right\}.$$

显然, $C\cup F^2\subseteq T, T+T\subseteq T$, 且 $T\cdot T\subseteq T$. 假若 $-1\in T$, 则 $-1=\sum_{i=1}^{n}c_ia_i^2(1-\eta_i)$, 其中 $c_i\in C$, $a_i\in F$, $\eta_i\in M_v$, $i=1,\cdots,n$. 记 $a_0:=1$, 设 $v(a_k)=\min\{v(a_i)\mid i=0,1,\cdots,n\}$, $0\leqslant k\leqslant n$, 且令 $b_i=a_ia_k^{-1}\in M_v$, $i=0,1,\cdots,n$. 由前面的等式有, $b_0^2+\sum_{i=1}^{n}c_ib_i^2(1-\eta_i)=0$, 即 $\bar{b}_0^2+\sum_{i=1}^{n}\bar{c}_i\bar{b}_i^2=0$, 这里 $\bar{z}:=z+M_v\in A_v/M_v$, 对于每个 $z\in A_v$. 当 $k=0$ 时, 有 $-1=-\bar{b}_0^2=\sum_{i=1}^{n}\bar{c}_i\bar{b}_i^2\in P_v$, 矛盾. 当 $k\neq 0$ 时, 有 $-\bar{b}_k^2=\bar{b}_0^2+\sum_{i\neq k}\bar{c}_i\bar{b}_i^2\in P_v$, 矛盾. 从而 $-1\notin T$. 因而, T 是域的一个亚正锥. 由定理 1.1.2 的推论, F 有一个正锥 P, 使得 $T\subseteq P$.

显然, $1+M_v\subseteq T\subseteq P$. 由命题 3.1.3 知, v 与 P 相容. 根据上面的推论 1 进一步可知, P_v 恰好为由 P 在 A_v/M_v 上所诱导的正锥. 证毕.

设 v 是域 F 的一个赋值，$\leqslant_v$ 是 A_v/M_v 的一个序，且 P_v 是 $\leqslant_v$ 的对应正锥. 根据上面的推论 2, P_v 可以提升为 F 的一个正锥 P, 使得 v 与 P 相容，且 P_v 恰好为由 P 在 A_v/M_v 上所诱导的正锥. 记 $\leqslant$ 为 P 的对应序，则 v 与 $\leqslant$ 相容，且 $\leqslant_v$ 恰好为由 $\leqslant$ 在 A_v/M_v 上所诱导的序.

定理 3.1.4 设 v 是域 F 的一个赋值，则 v 是一个实赋值，当且仅当 v 与 F 的某个序相容.

证明 设 v 与 F 的一个序 $\leqslant$ 相容，且令 P 为序 $\leqslant$ 的对应正锥. 由命题 3.1.3 的推论 1 知，P 诱导出剩余域 A_v/M_v 的一个正锥 P_v. 因而，剩余域 A_v/M_v 必是一个实域，即 v 是一个实赋值.

反过来，设 v 是一个实赋值，则剩余域 A_v/M_v 是一个实域. 由定理 1.1.3 知，剩余域 A_v/M_v 有一个正锥 P_v. 由命题 3.1.3 的推论 2 知，P_v 可以提升为 F 的一个正锥 P, 使得 v 与 P 相容. 此时，v 与序 $\leqslant_P$ 相容. 证毕.

作为上面有关概念和结果的一种推广，可以在亚序域的范畴中进行相应的讨论.

定义 3.1.4 设 (F,T) 是一个亚序域，v 是 F 的一个赋值. 称 v 与 T 相容 (或称 T 与 v 相容), 如果对于任意 $t_1, t_2 \in T$, $v(t_1+t_2) = \min\{v(t_1), v(t_1)\}$.

对于域 F 的一个亚正锥 T, 我们可规定 F 上一个二元关系 $\leqslant_T$ 如下：$a \leqslant_T b$ 当且仅当 $b-a \in T$. 易知 $\leqslant_T$ 是 F 的一个偏序. 此时，定义 3.1.4 有如下等价形式：F 的一个赋值 v 与 T 相容，如果由关系式 $0 <_T a \leqslant_T b$ 可推出 $v(a) \geqslant v(b)$.

现在，上面的命题 3.1.3 可推广如下.

定理 3.1.5 设 (F,T) 是一个亚序域，v 是 F 的一个赋值，则下列叙述等价：

(1) v 与 T 相容;

(2) A_v 关于 $\leqslant_T$ 是凸的，即由关系式 $0 \leqslant_T a \leqslant_T b \in A_v$, 可推出 $a \in A_v$;

(3) M_v 关于 $\leqslant_T$ 是凸的;

(4) v 与 (F,T) 的某个序相容.

证明 (1) $\Longrightarrow$ (2): 设 $0 \leqslant_T a \leqslant_T b \in A_v$, 则 a, $b-a \in T$. 由定义 3.1.4 知，$v(a) \geqslant \min\{v(a), v(b-a)\} = v(a+(b-a)) = v(b) \geqslant 0$. 从而 $a \in A_v$.

(2) $\Longrightarrow$ (3): 设 $0 \leqslant_T a \leqslant_T b \in M_v$. 当 $a=0$ 时，显然 $a \in M_v$. 当 $a \neq 0$ 时，则 $0 <_T b^{-1} \leqslant_T a^{-1}$. 由于 $b^{-1} \notin A_v$, 从而由叙述 (2) 知，$a^{-1} \notin A_v$, 即 $a \in M_v$.

(3) $\Longrightarrow$ (4): 作 F 的如下子集:

$$T_1 = \left\{ \sum_{i=1}^{n} t_i(1+\eta_i) \mid t_i \in T,\ \eta_i \in M_v,\ i=1,\cdots,n \right\}.$$

易知 $T \subseteq T_1$, $T_1+T_1 \subseteq T_1$, 且 $T_1 \cdot T_1 \subseteq T_1$. 假若 $-1 \in T_1$, 则 $-1 = \sum\limits_{i=1}^{n} t_i(1+\eta_i)$, 其中

$t_i \in T$, $\eta_i \in M_v$, $i=1,\cdots,n$. 记 $t_0=1\in T$, 且令 $v(t_k)=\min\{v(t_i)\mid i=0,1,\cdots,n\}$, $0\leqslant k\leqslant n$, 则必有 $t_k\neq 0$. 再令 $a_i=t_it_k^{-1}$, $i=0,1,\cdots,n$, 则 $a_i\in T$ 且 $a_i\in A$, $i=0,1,\cdots,n$. 显然仍有 $a_0+\sum\limits_{i=1}^n a_i(1+\eta_i)=0$. 从而 $a_0+\sum\limits_{i=1}^n a_i=-\sum\limits_{i=1}^n a_i\eta_i\in M_v$. 此时有 $0\leqslant_T 1=a_k\leqslant_T a_0+\sum\limits_{i=1}^n a_i\in M_v$. 由叙述 (3) 知, $1\in M_v$, 矛盾. 因而, T_1 是域 F 的一个亚正锥. 由定理 1.1.2 的推论知, F 有一个序 $\leqslant$, 它的正锥 P 包含 T_1.

现设 $\eta\in M_v$, 则由 T_1 的构造, $1-\eta\in T_1\subseteq P$. 从而 $\eta\leqslant 1$. 由于 $\eta\neq 1$, 从而进一步有 $\eta<1$. 由命题 3.1.3 知, v 与 (F,T) 的序 $\leqslant$ 相容.

(4) $\Longrightarrow$ (1): 设 v 与 (F,T) 的一个序 $\leqslant$ 相容, 且令 P 是 $\leqslant$ 的对应正锥, 则 $T\subseteq P$. 对于 $t_1,t_2\in T$, 显然有 $0\leqslant t_i\leqslant t_1+t_2$, $i=1,2$. 由于 v 与 $\leqslant$ 相容, 从而 $v(t_i)\geqslant v(t_1+t_2)$, $i=1,2$. 这表明: $\min\{v(t_1),v(t_2)\}\geqslant v(t_1+t_2)$. 显然, $\min\{v(t_1),v(t_2)\}\leqslant v(t_1+t_2)$. 因而, $\min\{v(t_1),v(t_2)\}=v(t_1+t_2)$. 由定义 3.1.4 知, v 与 T 相容. 证毕.

同样, 由定理 3.1.5, 可推出下面事实:

推论 设 v 是域 F 的一个赋值, T 是域 F 的一个亚正锥, 则 v 与 T 相容, 当且仅当 T 在剩余域 A_v/M_v 上所诱导的子集

$$T_v:=\{\bar{a}=a+M_v\mid a\in T\cap A_v\}$$

是 A_v/M_v 的一个亚正锥.

证明 显然, 无论 v 是否与 T 相容, 总有 $T_v+T_v\subseteq T_v$, $T_v\cdot T_v\subseteq T_v$, 且 $(A_v/M_v)^2\subseteq T_v$.

设 v 与 T 相容. 由定理 3.1.5 知, v 与亚序域 (F,T) 的某个正锥 P 相容. 根据命题 3.1.3 的推论 1, P 在 A_v/M_v 上诱导出一个正锥 P_v, 使得 $P_v=\{\bar{a}\mid a\in P\cap A_v\}$. 注意到 $T\subseteq P$, 即有 $T_v\subseteq P_v$. 从而 $-1\notin T_v$. 由定义 1.1.4 知, T_v 是 A_v/M_v 的一个亚正锥.

现设 T_v 是 A_v/M_v 的一个亚正锥. 假若 v 与 T 不相容, 则由定理 3.1.5 知, A_v 关于 $\leqslant_T$ 不是凸的. 从而对于某两个 $a,b\in F$, 有 $0\leqslant_T a\leqslant_T b\in A_v$, 但 $a\notin A_v$. 于是 $a^{-1}\in M_v$, 且 $1\leqslant_T ba^{-1}$. 由此有 $ba^{-1}-1\in T$, 进而有 $-1=\overline{ba^{-1}-1}\in T_v$, 矛盾. 因此, v 与 T 相容. 证毕.

§3.2　实赋值的构造与拓展

在本节中, 将先考虑域的实赋值的构造形式, 然后研究实赋值在扩域上的拓展. 由上节中定理 3.1.4 知, 实赋值总与域的某个序相容. 因此, 关于实赋值构造

的研究可以针对域的一个特定的序，而讨论与该序相容的实赋值的形式.

设 $\leqslant$ 是域 F 的一个序，且 E 是 F 的一个子域，现在域 F 上规定如下二元关系 $\sim$:

$$a \sim b, \text{当且仅当有非零 } e_1,\, e_2 \in E, \text{使得 } |a| \leqslant e_1|b| \text{ 且 } |b| \leqslant e_2|a|.$$

容易验证：$\sim$ 是 F 上的一个等价关系. 对于 $a \in F$, 用 $[a]_{(E,\leqslant)}$ 表示对于所规定的等价关系 $\sim$ 元素 a 所在的等价类. 为简单起见，在不致于引起混淆的前提下，等价类 $[a]_{(E,\leqslant)}$ 简记为 $[a]$. 如此所得的等价类 $[a]$ 称作 a 关于 $\leqslant$ 的 E- 阿基米德类 . 显然，对于任意 $a \in F$ 以及任意非零 $e \in E$, $[a] = [ea]$.

作集合 $\Gamma := \{[a] \mid a \in F \text{ 且 } a \neq 0\}$, 且对于 $[a], [b] \in \Gamma$, 规定： $[a] + [b] = [ab]$.

若 $[a] = [c]$, $[b] = [d]$, 则有非零 e_1, e_2, e_3 和 $e_4 \in E$, 使得 $|a| \leqslant e_1|c|$, $|c| \leqslant e_2|a|$, $|b| \leqslant e_3|d|$ 且 $|d| \leqslant e_4|b|$. 从而 $|ab| \leqslant (e_1e_3)|cd|$, 且 $|cd| \leqslant (e_2e_4)|ab|$. 这表明 $[ab] = [cd]$. 因此，上面的规定是合理的.

进一步可验证： Γ 关于所规定的运算 + 组成一个 Abel 群，其零元为 $[1]$, 且对于 $[a] \in \Gamma$, $[a]$ 的负元为 $[a^{-1}]$.

为赋予群 Γ 一个序结构，在 Γ 上规定如下仍记作 $\leqslant$ 的二元关系：

$$[a] < [b], \text{当且仅当 } [a] \neq [b], \text{且对于 } F \text{ 的序} \leqslant, |b| < |a|.$$

设 $[a] \neq [b]$, 其中 $|b| < |a|$. 假若对于某个 $c \in [a]$ 以及某个 $d \in [b]$, $|c| \leqslant |d|$. 由等价类的规定知，有 $e_1, e_2 \in E$, 使得 $|a| \leqslant e_1|c|$, 且 $|d| \leqslant e_2|b|$, 从而有 $|a| \leqslant (e_1e_2)|b|$. 由此知 $a \sim b$, 即 $[a] = [b]$, 矛盾. 因而，对于每个 $c \in [a]$ 和每个 $d \in [b]$, 均有 $|d| < |c|$. 因此， $\leqslant$ 的规定是合理的.

由上面的规定和讨论，可断言：对于 $[a]$, $[b] \in \Gamma$, $[a] \leqslant [b]$ 当且仅当有非零 $e \in E$, 使得 $|b| \leqslant e|a|$. 事实上，若有 $e \in E$, 使得 $|b| \leqslant e|a|$, 则 $e > 0$, 且当 $[b] \neq [ea]$ 时， $[ea] < [b]$ 即 $[a] < [b]$. 因而 $[a] \leqslant [b]$. 反过来，若 $[a] \leqslant [b]$, 则 $[a] = [b]$ 或 $[a] < [b]$, 从而有非零 $e \in E$, 使得 $|b| \leqslant e|a|$, 或者 $|b| < |a|$.

借助于上面断言，易证所规定的 $\leqslant$ 是群 Γ 的一个序. 于是，我们得到一个序群 $(\Gamma, \leqslant)$.

再作 F 到 $\Gamma \cup \{\infty\}$ 的如下映射：

$$v:\quad a \longmapsto \begin{cases} \infty, & \text{若 } a = 0, \\ [a], & \text{若 } a \neq 0, \end{cases} \qquad a \in F.$$

由定义可验证： v 是域 F 的一个赋值.

设 $0 < a \leqslant b$. 当 $[a] = [b]$ 时，显然 $v(a) = v(b)$; 而当 $[a] \neq [b]$ 时，由 Γ 的序 $\leqslant$ 的规定， $v(a) = [a] > [b] = v(b)$. 由定义 3.1.2 知， v 与域 F 的序 $\leqslant$ 相容. 根据定

理 3.1.4, v 是域 F 的一个实赋值.

现考察 v 的赋值环 A_v. 注意到, $a \in A_v \iff v(a) \geqslant [1]$, 即 $a = 0$ 或 $[a] \geqslant [1] \iff$(根据上面断言) 有非零 $e \in E$, 使得 $|a| \leqslant e$. 从而 $A_v = \{a \in F \mid$ 有非零 $e \in E$, 使得 $|a| \leqslant e\}$, 即 A_v 是子域 E 关于 $\leqslant$ 的凸包. 子域 E 关于序 $\leqslant$ 的凸包特记作 $A(E, \leqslant)$.

定义 3.2.1 如上规定的实赋值 v 称作关于子域 E 和序 $\leqslant$ 的典型实赋值，且记作 $v_{(E,\leqslant)}$. 而相应的赋值环 $A(E, \leqslant)$ 称作关于子域 E 和序 $\leqslant$ 的典型实赋值环．特别地，当 $E = \mathbb{Q}$ 时， $v_{(\mathbb{Q},\leqslant)}$ 简称为关于序 $\leqslant$ 的典型实赋值，而 $A(\mathbb{Q}, \leqslant)$ 简称为关于序 $\leqslant$ 的典型实赋值环．

对于域 F 的正锥 P 和子域 E, 关于 E 和序 $\leqslant_P$ 的典型实赋值和典型实赋值环将分别径称为关于 E 和 P 的典型实赋值和典型实赋值环，且分别记作 $v_{(E,P)}$ 和 $A(E, P)$.

下面的重要定理表明：在赋值等价的意义下，每一个实赋值恰好为如上规定的典型实赋值. 在证明定理之前，我们先证明下面的引理.

引理 3.2.1 设 v 是域 F 的一个实赋值， A 和 M 分别是 v 的赋值环和赋值理想，则 $\mathbb{Q} \subseteq A$. 如果 E 是 F 的一个包含在 A 中的极大子域，则剩余域 A/M 是 E 一个代数扩张，只要认定 $E = E + M/M \subseteq A/M$.

证明 由命题 3.1.2 的推论 2 知， F 是一个实域，即有 $\mathbb{Q} \subseteq F$. 对于每个正整数 n, 由命题 3.1.2 知， $v(n) = v(1^2 + \cdots + 1^2) = v(1^2) = 0$. 这表明 n 是 A 中可逆元. 由此可知，每个正有理数属于 A. 因而有， $\mathbb{Q} \subseteq A$.

由于 $E + M/M \cong E/E \cap M = E$, 从而可认定 $E = E + M/M \subseteq A/M$. 设 $\bar{\alpha} = \alpha + M$ 为 A/M 中任意元素，其中 $\alpha \in A$. 当 $\alpha \in E$ 时， $\bar{\alpha} \in E + M/M = E$. 下设 $\alpha \notin E$. 由 E 的极大性知， $E[\alpha]$ 中至少有一个非零元素在 A 中不可逆；否则 $E(\alpha) \subseteq A$. 从而 $E[\alpha] \cap M \neq \{0\}$. 于是有

$$0 \neq a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n \in M,$$

其中 $a_0, a_1, \cdots, a_n \in E$, 且 $a_0 \neq 0$. 由于 $E \cap M = \{0\}$, 从而 $n \geqslant 1$.

由上式知，在剩余域 A/M 中 $a_0\bar{\alpha}^n + a_1\bar{\alpha}^{n-1} + \cdots + a_n = 0$. 这表明 $\bar{\alpha}$ 是 E 上代数元. 因此， A/M 是 E 的代数扩张. 证毕.

定理 3.2.2 设 v 是域 F 的赋值，则下列叙述等价：

(1) v 是一个实赋值;

(2) v 的赋值环是典型实赋值环 $A(E, \leqslant)$, 这里 $\leqslant$ 是 F 的一个序， E 是 F 的一个子域;

(3) v 等价于典型实赋值 $v_{(E,\leqslant)}$, 这里 $\leqslant$ 是 F 的一个序， E 是 F 的一个子域.

证明 (1) $\Longrightarrow$ (2): 设 A 是 v 的赋值环. 由引理 3.2.1 知, $\mathbb{Q}\subseteq A$. 借助于 Zorn 引理, A 包含 F 的一个极大子域 E. 对于 $\alpha\in A$, 由引理 3.2.1 知, $\bar{\alpha}=\alpha+M$ 是 E 上代数元, 这里 M 为 v 的赋值理想. 于是在剩余域 A/M 中,

$$\bar{\alpha}^n+a_1\bar{\alpha}^{n-1}+\cdots+a_n=0,$$

其中 $a_1,\cdots,a_n\in E$.

从而有 $\eta:=\alpha^n+a_1\alpha^{n-1}+\cdots+a_n\in M$. 根据定理 3.1.4, F 有一个序 $\leqslant$, 使得 v 与 $\leqslant$ 相容. 由定理 2.4.5 的推论 1 知, $|\alpha|<1+|a_1|+\cdots+|a_{n-1}|+|a_n-\eta|\leqslant 1+|a_1|+\cdots+|a_{n-1}|+|a_n|+|\eta|$. 再由命题 3.1.3 知, $|\eta|<1$. 从而 $|\alpha|<e$, 这里 $e:=2+|a_1|+\cdots+|a_{n-1}|+|a_n|\in E$. 因而, $\alpha\in A(E,\leqslant)$, 即有 $A\subseteq A(E,\leqslant)$.

反过来, 对于 $\alpha\in A(E,\leqslant)$, 有 $e\in E$, 使得 $|\alpha|\leqslant e$. 由于 $E\subseteq A$, 从而有 $0\leqslant|\alpha|\leqslant e\in A$. 根据命题 3.1.3, A 关于 $\leqslant$ 是凸的. 因而有 $|\alpha|\in A$, 即有 $\alpha\in A$. 由 α 的任意性, $A(E,\leqslant)\subseteq A$. 因此, $A=A(E,\leqslant)$.

(2) $\Longrightarrow$ (3): 由条件和前面的讨论知, v 和 $v_{(E,\leqslant)}$ 有相同的赋值环 $A(E,\leqslant)$. 因此, v 和 $v_{(E,\leqslant)}$ 等价.

(3) $\Longrightarrow$ (1): 由叙述 (3) 知, v 和 $v_{(E,\leqslant)}$ 有相同的赋值环, 从而有相同的剩余域. 由上面讨论知, $v_{(E,\leqslant)}$ 是一个实赋值, 即该剩余域是实域. 这表明: v 是一个实赋值. 证毕.

推论 1 设 v 是域 F 的一个赋值, $\leqslant$ 是 F 的一个序, 则 v 与 $\leqslant$ 相容, 当且仅当 F 有一个子域 E, 使得 v 的赋值环为 $A(E,\leqslant)$.

推论 2 设 v 是域 F 的一个实域值, 且它的赋值环 $A_v=A(E,\leqslant)$, 其中 $\leqslant$ 是 F 的一个序, E 是 F 的一个子域, 则 $\leqslant$ 在剩余域 A_v/M_v 上所诱导的序是在 E 上的阿基米德序.

证明 显然, $A_v=A(E,\leqslant)$ 关于序 $\leqslant$ 是凸的. 由命题 3.1.3 知, v 与序 $\leqslant$ 相容. 根据命题 3.1.3 的推论 1, $\leqslant$ 在剩余域 A_v/M_v 上诱导出一个序 $\leqslant_v$, 使得对于每个 $a\in A_v$, $0\leqslant_v\bar{a}:=a+M_v$, 只要 $0\leqslant a$.

对于每个 $\bar{a}=a+M_v\in A_v/M_v$, 其中 $a\in A_v$, 由 $A_v=A(E,\leqslant)$ 的结构知, 有非零 $e\in E$, 使得 $|a|\leqslant e$, 即 $0\leqslant e-|a|$. 由此有 $0\leqslant_v\overline{e-|a|}=e-|\bar{a}|$. 从而有 $|\bar{a}|\leqslant_v e$. 这表明: A_v/M_v 对于序 $\leqslant_v$ 没有在 E 上的无限大元素. 因此, $\leqslant_v$ 是在 E 上的阿基米德序. 证毕.

推论 3 设 $\leqslant$ 是域 F 的一个序, 则 F 的全体与 $\leqslant$ 相容的实赋值环对于集合的包含关系组成的一个链, 其中最小成员为 $A(\mathbb{Q},\leqslant)$.

证明 设 A_1 和 A_2 是 F 的任意两个与 $\leqslant$ 相容的实赋值环, 且 $A_1\not\subseteq A_2$, 则有 $a\in A_1$, 使得 $a\notin A_2$. 由定理 3.2.2, 可令 $A_2=A(E,\leqslant)$, 其中 E 是 $\mathbb{Q}$ 和 F 的一个中间域. 此时 $a\notin A(E,\leqslant)$, 即对于每个非零 $e\in E$, 都有 $|a|>e$. 设 z 是 A_2 中任意

元素，则有某个非零 $e_1 \in E$, 使得 $|z| \leqslant e_1$. 从而有 $0 \leqslant |z| < |a| \in A_1$. 由于 A_1 关于序 $\leqslant$ 是凸的，从而 $|z| \in A_1$, 即有 $z \in A_1$. 因而， $A_2 \subseteq A_1$. 这表明： F 的全体与 $\leqslant$ 相容的赋值环对于集合的包含关系组成一个链.

对于每个与 $\leqslant$ 相容的赋值 v, $A_v = A(E, \leqslant)$, 其中 E 是 F 的一个子域. 由于 $\mathbb{Q} \subseteq E$, 从而 $A(\mathbb{Q}, \leqslant) \subseteq A(E, \leqslant) = A_v$. 证毕.

此外，由定理 3.2.2 容易建立下面事实：

命题 3.2.3 序域 $(F, \leqslant)$ 是一个非阿基米德序域，当且仅当 F 有一个非浅显的赋值与 $\leqslant$ 相容.

证明 设 $\leqslant$ 是 F 的一个非阿基米德序，则 F 中有在 $\mathbb{Q}$ 上的无限大元素. 令 $A(\mathbb{Q}, \leqslant)$ 是关于 $\leqslant$ 的典型实赋值环. 显然， $A(\mathbb{Q}, \leqslant)$ 不包含在 $\mathbb{Q}$ 上的无限大元素，即 $A(\mathbb{Q}, \leqslant) \neq F$. 这表明典型实赋值 $v_{(\mathbb{Q}, \leqslant)}$ 是非浅显的.

现设 v 是 F 的一个非浅显赋值，且 v 与 $\leqslant$ 相容. 由定理 3.2.2 知， v 的赋值环为 $A(E, \leqslant)$, 其中 E 是 F 的一个子域. 由于 v 是非浅显的，从而 $A(E, \leqslant) \neq F$. 对于任意取出的 $\alpha \in F \setminus A(E, \leqslant)$, 由 $A(E, \leqslant)$ 中元素的特性知，对于每个 $e \in E$, $e < |\alpha|$. 注意到， $\mathbb{Q} \subseteq E$. 从而对于每个 $q \in \mathbb{Q}$, $q < |\alpha|$, 即 α 是在 $\mathbb{Q}$ 上的无限大元素. 因此， $\leqslant$ 是一个非阿基米德序. 证毕.

结合定理 3.2.2 和命题 3.2.3 可得出这样一个事实：一个实域仅有浅显实赋值，当且仅当它的每个序都是阿基米德序.

由赋值的拓展定理知，任何一个赋值在扩域上都有拓展. 自然会问：任何一个实赋值在实扩域上是否有实拓展？下面例子说明，这一问题的回答是否定的.

例 1 设 R 是一个实闭域， $F = R(t)$, 其中 t 是 R 上的一个超越元，且 v 是 F 的这样一个赋值，使得对于每个非零多项 $f(t) \in R[t]$, $v(f(t)) = -\deg f(t)$. 由命题 3.1.3 知，剩余域 $F_v \cong R$. 从而， v 是 F 上的一个实赋值. 令 $K = F(\sqrt{t^{-1}-1})$, 这里 $\sqrt{t^{-1}-1}$ 表示多项式 $x^2 - (t^{-1} - 1)$ 在 F 的代数闭包中的一个根. 显然， $K = R(\sqrt{t^{-1}-1})$ 是 R 的单超越扩张. 因而， K 是 F 的一个实扩张.

假若 v 可拓展为 K 的一个实赋值 w, 则由定理 3.1.4 知， w 与 K 的一个序 $\leqslant$ 相容. 注意到 $t^{-1} - 1 = (\sqrt{t^{-1}-1})^2 > 0$, 即 $0 < 1 < t^{-1}$. 然而 $w(1) = 0 < 1 = v(t^{-1}) = w(t^{-1})$, 矛盾于 w 与 $\leqslant$ 的相容性.

下面定理给出一个实赋值在扩域上有实拓展的充分必要条件.

定理 3.2.4 设 v 是域 F 的一个实赋值， K 是 F 的一个扩张，则 v 可拓展为 K 的一个实赋值，当且仅当 K 有一个序 $\leqslant$, 使得 v 与 $\leqslant$ 在 F 上的限制相容.

证明 设 v 可拓展为 K 的一个实赋值 w. 由定理 3.1.4 知， w 与 K 的一个序 $\leqslant$ 相容. 记 $\leqslant_F$ 为序 $\leqslant$ 在 F 上的限制，则由定义 3.1.2 可知， v 与 $\leqslant_F$ 相容.

反过来，设 K 有一个序 $\leqslant$, 使得 v 与 $\leqslant_F$ 相容，这里 $\leqslant_F$ 表示序 $\leqslant$ 在 F 上的限制. 根据定理 3.2.2 的推论 1 知，对于 F 的某个子域 E, v 的赋值环为 $A_v = A(E, \leqslant_F)$.

据此，我们有域 K 的典型实赋值 $v_{(E,\leqslant)}$, 使得 $v_{(E,\leqslant)}$ 的赋值环为 $A(E,\leqslant)$. 显然, $A(E,\leqslant)\cap F=A(E,\leqslant_F)$. 因此， $v_{(E,\leqslant)}$ 是 v 在 K 上的一个实拓展. 证毕.

定理 3.2.5 设 v 是域 F 的一个赋值， $\leqslant$ 是 F 的一个序，则 v 与 $\leqslant$ 相容，当且仅当 v 可惟一地拓展为序域 $(F,\leqslant)$ 的实闭包的一个实赋值.

证明 用 R 表示序域 $(F,\leqslant)$ 的实闭包，且 $\leqslant_{R^2}$ 表示 R 的惟一序. 显然， $\leqslant$ 是 $\leqslant_{R^2}$ 在 F 上的限制.

设 v 与 $\leqslant$ 相容，则由定理 3.2.4 知， v 可拓展为 R 的一个实赋值 w. 下证 w 的惟一性. 设 A_v 和 M_v 分别为 v 的赋值环和赋值理想. 根据定理 3.2.2 的推论 1, 可令 $A_v=A(E,\leqslant)$, 其中 E 为 F 的一个子域. 设 B_w 和 M_w 分别是 w 的赋值环和赋值理想，则 B_w/M_w 是 A_v/M_v 的一个代数扩张. 对于 $b\in B_w$, $\bar{b}:=b+M_w$ 是 A_v/M_v 上代数元，即有

$$\bar{b}^n+\bar{a}_1\bar{b}^{n-1}+\cdots+\bar{a}_n=0,$$

其中 $a_1,\cdots,a_n\in A_v$.

根据定理 3.1.4 和命题 3.1.3 的推论知， w 必与 R 的惟一序 $\leqslant_{R^2}$ 相容，且 $\leqslant_{R^2}$ 在剩余域 B_w/M_w 上诱导出一个序 $\leqslant_w$. 由定理 2.4.5 的推论 1 知， $\overline{|b|}=|\bar{b}|<_w 1+|\bar{a}_1|+\cdots+|\bar{a}_n|=\overline{1+|a_1|+\cdots+|a_n|}$. 由序 $\leqslant_w$ 的规定有, $|b|\leqslant_{R^2}1+|a_1|+\cdots+|a_n|\in A_v$. 由于 $A_v=A(E,\leqslant)$, 从而有 $e\in E$, 使得 $1+|a_1|+\cdots+|a_n|\leqslant e$. 于是有 $|b|\leqslant_{R^2}e$, 即 $b\in A(E,\leqslant_{R^2})$. 由 b 的任意性知， $B_w\subseteq A(E,\leqslant_{R^2})$. 反过来，对于每个 $b\in A(E,\leqslant_{R^2})$, 有 $e\in E$, 使得 $|b|\leqslant_{R^2}e$. 此时有 $0\leqslant_{R^2}|b|\leqslant_{R^2}e\in E\subseteq A_v\subseteq B_w$. 再由命题 3.1.3 知， B_w 关于 $\leqslant_{R^2}$ 是凸的. 从而 $|b|\in B_w$, 即 $b\in B_w$. 因此， $B_w=A(E,\leqslant_{R^2})$. 这表明： w 等价于关于子域 E 和序 $\leqslant_{R^2}$ 的典型实赋值. 必要性获证.

现设 v 可拓展为 R 的一个实赋值 w. 由定理 3.1.4, w 与 $\leqslant_{R^2}$ 相容. 若 $0<a\leqslant b$ 即 $0<_{R^2}a\leqslant_{R^2}b$, 其中 $a,b\in F$, 则 $w(a)\geqslant w(b)$, 即 $v(a)\geqslant v(b)$. 由定义 3.1.2 知, v 与 $\leqslant$ 相容. 证毕.

设 v 是域 F 的一个实赋值，且用 $\mathcal{X}_F^v$ 表示 F 的所有与 v 相容的序 (正锥) 组成的集合. 由定理 3.1.4 知， $\mathcal{X}_F^v$ 是 F 的序空间 $\mathcal{X}_F$ 的非空子集. 设 $P\in\mathcal{X}_F$, 但 $P\notin\mathcal{X}_F^v$. 由命题 3.1.3 可知，存在某个 $a\in M_v$, 使得 $1<_P a$. 这样， $P\in H(a-1)$, 但 $H(a-1)\cap\mathcal{X}_F^v=\phi$. 因而， $\mathcal{X}_F^v$ 是序空间 $\mathcal{X}_F$ 的闭子集. 因此， $\mathcal{X}_F^v$ 对于子空间拓扑也是一个 Hausdorff 的和全不连通的紧空间.

根据定理 2.1.6, 立即有下面的结果.

命题 3.2.6 设 v 是域 F 的一个实赋值， K 是 F 的一个扩张，且 w 是 v 在 K 上的一个实拓展，则从 $\mathcal{X}_K^w$ 到 $\mathcal{X}_F^v$ 的限制映射 r: $Q\longmapsto Q\cap F$ 是一个连续的闭映射.

§3.3 实 位

在赋值论中，另一个与赋值和赋值环密切相关的概念是域的位. 设 F 和 L 都是域，且 ∞ 是一个独立的符号. F 的一个 L- 值位是域 F 到 $L\cup\{\infty\}$ 的一个映射 ϕ, 使得下列条件成立： (1) 集 $A_\phi := \{a\in F \mid \phi(a)\in L\}$ 是 F 的一个子环； (2)ϕ 在 A_ϕ 上的限制 $\phi\mid_{A_\phi}$ 是 A_ϕ 到 L 的一个环同态； (3) 若 $\phi(a)=\infty$, 则 $\phi(a^{-1})=0$. F 的一个 L- 值位也称作域 F 到 L 的一个位. 由此可知， A_ϕ 是 F 的一个赋值环，相应的赋值理想 $M_\phi=\{a\in F \mid \phi(a)=0\}$, 可逆元群 $U_\phi=\{a\in F \mid \phi(a)\neq 0$ 且 $\phi(a)\neq\infty\}$. 因而， A_ϕ, M_ϕ, U_ϕ 和 A_ϕ/M_ϕ 分别称作位 ϕ 的赋值环，赋值理想，可逆元群和剩余域.

根据域 L 是否是实域，自然产生如下定义.

定义 3.3.1 设 ϕ 是域 F 到 L 的一个位. 若 L 是一个实域，则称 ϕ 是一个实位 .

对于域 F 的一个 L- 值位 ϕ, ϕ 诱导出剩余域 A_ϕ/M_ϕ 到 L 的一个嵌入，从而 A_ϕ/M_ϕ 可看做 L 的一个子域. 因而，当 ϕ 是实位时， A_ϕ/M_ϕ 是一个实域，即 A_ϕ 是 F 的一个实赋值环. 此外，当 ϕ 是满射即 $\phi(A_\phi)=L$ 时， $A_\phi/M_\phi\cong L$. 此时, ϕ 是实位，当且仅当 A_ϕ 是 F 的一个实赋值环. 因此，前两节中关于实赋值和实赋值环的有关概念与结论在实位的讨论中有相应的形式.

由刚才的讨论以及命题 3.1.2 的推论 2, 立即可建立如下事实：

命题 3.3.1 (1) 若 ϕ 是域 F 的一个实位，则 ϕ 的赋值环是 F 的一个实赋值环，且 F 是一个实域.

(2) 对于域 F 的一个 L- 值位 ϕ, 其中 ϕ 是满射，则 ϕ 是 F 的一个实位，当且仅当 A_ϕ 是 F 的一个实赋值环.

设 A 是域 F 的一个赋值环， M 是 A 的赋值理想， $\overline{F}:=A/M$ 是 A 的剩余域，则有 F 的一个 $\overline{F}$- 值位 ϕ_A, 使得对于 $a\in F$, $\phi_A(a)=a+M$, 当 $a\in A$ 时；否则， $\phi_A(a)=\infty$. 在赋值论中，这样的位 ϕ_A 称作由赋值环 A 所确定的正规位. 由命题 3.3.1(2) 知，正规位 ϕ_A 是实位，当且仅当赋值环 A 是域 F 的一个实赋值环.

设 $\leqslant$ 是域 F 的一个序， E 是 F 的一个子域. 由定理 3.2.2 知， $A(E,\leqslant)$ 是 F 的一个实赋值环，从而正规位 $\phi_{A(E,\leqslant)}$ 是 F 的一个实位. 这样所得的正规位称作关于子域 E 和序 $\leqslant$ 的典型实位，且记作 $\phi_{(E,\leqslant)}$.

对于域 F 的一个序 $\leqslant$, 由上面途径可得到 F 的典型实位 $\phi_{(\mathbb{Q},\leqslant)}$. 设 $\overline{F}$ 是实位 $\phi_{(\mathbb{Q},\leqslant)}$ 的剩余域. 由定理 3.2.2 的推论 2, $\leqslant$ 在 $\overline{F}$ 上诱导出一个阿基米德序 $\bar{\leqslant}$. 由定理 1.4.4 知，存在惟一的 $(\overline{F},\bar{\leqslant})$ 到实数域 $\mathbb{R}$ 的保序嵌入 π. 将 $\phi_{(\mathbb{Q},\leqslant)}$ 与 π 合成，即得到 F 的一个 $\mathbb{R}$- 值位. 如此得到的 $\mathbb{R}$- 值位称作关于序 $\leqslant$ 的典型 $\mathbb{R}$- 值位，且记作 $\phi_\leqslant$.

为了引进位与序的相容性，我们给出下面的定义.

定义 3.3.2 设 ϕ 是域 F 的一个 L- 值位，且 $\leqslant_F$ 和 $\leqslant_L$ 分别为 F 和 L 的序. 称 ϕ 与序 $\leqslant_F$ 和 $\leqslant_L$ 相容，若由关系式 $0 \leqslant_F a \leqslant_F b$, 可推出 $\phi(b) = \infty$ 或 $0 \leqslant_L \phi(a) \leqslant_L \phi(b)$. 当 L 只有惟一序 (例如 L 是实闭域) 时，简称 ϕ 与序 $\leqslant_F$ 相容.

由上面定义可以验证：典型实位 $\phi_{(E,\leqslant)}$ 与序 $\leqslant$ 和序 $\bar{\leqslant}$ 相容，其中 $\bar{\leqslant}$ 是 $\leqslant$ 在 $A(E,\leqslant)$ 的剩余域上所诱导的序. 而典型 $\mathbb{R}$- 值位 $\phi_{\leqslant}$ 与序 $\leqslant$ 相容.

命题 3.3.2 设 ϕ 是域 F 的一个 L- 值位，且对于 F 的一个序 $\leqslant_F$ 以及 L 的一个序 $\leqslant_L$, ϕ 与 $\leqslant_F$ 和 $\leqslant_L$ 相容，则 ϕ 的赋值环 $A_\phi = A(E, \leqslant_F)$, 对于 F 的某个子域 E.

证明 根据定理 3.1.5 和定理 3.2.2 的推论 1, 只需证明： A_ϕ 关于序 $\leqslant_F$ 是凸的. 设 $0 \leqslant_F a \leqslant_F b \in A_\phi$, 则 $\phi(b) \neq \infty$. 由相容性有 $0 \leqslant_L \phi(a) \leqslant_L \phi(b)$. 这表明: $\phi(a) \neq \infty$, 即 $a \in A_\phi$. 因此， A_ϕ 关于 $\leqslant_F$ 是凸的. 证毕.

定理 3.3.3 设 ϕ 是域 F 的一个 L- 值位，则下列叙述等价:

(1) ϕ 是一个实位;

(2) L 是一个实域，且对于 L 的每个序 $\leqslant_L$, F 有一个序 $\leqslant_F$, 使得 ϕ 与 $\leqslant_F$ 和 $\leqslant_L$ 相容;

(3) F 有一个序 $\leqslant_F$, 且 L 有一个序 $\leqslant_L$, 使得 ϕ 与 $\leqslant_F$ 和 $\leqslant_L$ 相容.

证明 (1) $\Longrightarrow$ (2): 设 F_ϕ 是 ϕ 的剩余域，则 F_ϕ 同构于 L 的一个子域. 从而可认定 $F_\phi \subseteq L$. 设 $\leqslant_L$ 是 L 的任意一个序，且记 $\leqslant_\phi$ 是 $\leqslant_L$ 在 F_ϕ 上的限制. 由命题 3.3.1 知， ϕ 的赋值环 A_ϕ 是 F 的一个实赋值环. 由命题 3.1.3 的推论 2 知， F 有一个序 $\leqslant_F$, 使得 $\leqslant_F$ 与实赋值环 A_ϕ 相容 (即 A_ϕ 关于 $\leqslant_F$ 是凸的), 且 $\leqslant_\phi$ 恰为 $\leqslant_F$ 在 F_ϕ 上所诱导的序.

设 $0 \leqslant_F a \leqslant_F b$, 且 $\phi(b) \neq \infty$, 则有 $0 \leqslant_F a \leqslant_F b \in A_\phi$. 由于 A_ϕ 关于序 $\leqslant_F$ 是凸的, 从而 $a \in A_\phi$. 由于 $\leqslant_\phi$ 是 $\leqslant_F$ 在 F_ϕ 上所诱导的序, 从而有 $0 \leqslant_\phi \phi(a) \leqslant_\phi \phi(b)$, 即 $0 \leqslant_L \phi(a) \leqslant_L \phi(b)$. 这表明 ϕ 与序 $\leqslant_F$ 和 $\leqslant_L$ 相容.

(2) $\Longrightarrow$ (3): 显然.

(3) $\Longrightarrow$ (1): 由于 L 有序，从而 L 是实域. 因而， ϕ 是一个实位. 证毕.

推论 设 ϕ 是域 F 的一个 L- 值位，其中 L 是一个实闭域，则 F 有一个序 $\leqslant$, 使得 ϕ 与 $\leqslant$ 相容.

定理 3.3.4 设 ϕ 是域 F 的一个 L- 值位， $\leqslant_F$ 是域 F 的一个序，而 $\leqslant_L$ 是 L 的一个序，则 ϕ 与 $\leqslant_F$ 和 $\leqslant_L$ 相容，当且仅当 ϕ 的赋值环 A_ϕ 关于 $\leqslant_F$ 是凸的，且 ϕ 诱导出一个从序域 $(A_\phi/M_\phi, \leqslant_\phi)$ 到 $(L, \leqslant_L)$ 的保序嵌入，这里 $\leqslant_\phi$ 是 $\leqslant_F$ 在 A_ϕ/M_ϕ 上所诱导的序.

证明 设 ϕ 与 $\leqslant_F$ 和 $\leqslant_L$ 相容. 由命题 3.3.2 知, A_ϕ 关于 $\leqslant_F$ 是凸的. 显然, ϕ 诱导出 A_ϕ/M_ϕ 到 L 的一个嵌入 $\bar{\phi}$, 使得对于每个 $a \in A_\phi$, $\bar{\phi}(\bar{a}) = \phi(a)$, 其中 $\bar{a} := a + M_\phi \in A_\phi/M_\phi$. 设 $0 \leqslant_\phi \bar{a} \leqslant_\phi \bar{b}$, 其中 $\bar{a}, \bar{b} \in A_\phi/M_\phi$, 则由 $\leqslant_\phi$ 的规定知, $0 \leqslant_F a \leqslant_F b$. 显然 $\phi(b) \neq \infty$. 由 ϕ 与 $\leqslant_F$ 和 $\leqslant_L$ 的相容性, $0 \leqslant_L \phi(a) \leqslant_L \phi(b)$, 即 $0 \leqslant_L \bar{\phi}(\bar{a}) \leqslant_L \bar{\phi}(\bar{b})$. 因此, $\bar{\phi}$ 是一个保序嵌入.

充分性显然. 证毕.

对于实位的拓展, 可以建立如下结论.

定理 3.3.5 设 ϕ 是 F 的一个 L- 值位, 其中 L 是一个实闭域, K 是 F 的一个代数扩张, 则 ϕ 可以拓展为 K 的一个 L- 值位, 当且仅当 K 有一个序 $\leqslant$, 使得 ϕ 与 $\leqslant_F$ 相容, 这里 $\leqslant_F$ 是 $\leqslant$ 在 F 上的限制.

证明 设 K 有一个序 $\leqslant$, 使得 ϕ 与 $\leqslant$ 在 F 上的限制 $\leqslant_F$ 相容. 设 A_ϕ 是 ϕ 的赋值环, 则 A_ϕ 是 F 的一个实赋值环. 由命题 3.3.2 知, $A_\phi = A(E, \leqslant_F)$, 其中 E 是 K 的一个子域. 令 $B = A(E, \leqslant)$, 则 B 是 K 的一个与 $\leqslant$ 相容的实赋值环. 令 M_B 是 B 的赋值理想, 且 $\leqslant_B$ 是 $\leqslant$ 在剩余域 $F_B := B/M_B$ 上所诱导的序. 容易验证: $(F_B, \leqslant_B)$ 是序域 $(F_\phi, \leqslant_\phi)$ 的序扩张, 这里 F_ϕ 为 ϕ 的剩余域, $\leqslant_\phi$ 是 $\leqslant_F$ 在 F_ϕ 上所诱导的序. 由于 ϕ 与 $\leqslant_F$ 相容, 从而 ϕ 诱导出序域 $(F_\phi, \leqslant_\phi)$ 到 $(L, \leqslant_{L^2})$ 的一个保序嵌入, 这里 $\leqslant_{L^2}$ 表示 L 的惟一序. 据此可认定: $F_\phi \subseteq L$, 且 $\leqslant_\phi$ 是 $\leqslant_{L^2}$ 在 F_ϕ 上的限制. 令 R 是 F_ϕ 在 L 中的代数闭包. 由命题 2.1.5 可知, R 是序域 $(F_\phi, \leqslant_\phi)$ 的实闭包. 再令 R_1 是序域 $(F_B, \leqslant_B)$ 的实闭包. 注意到 F_B 是 F_ϕ 的代数扩张, 从而 R_1 也是序域 $(F_\phi, \leqslant_\phi)$ 的实闭包. 由实闭包的惟一性, 有 R_1 到 R 的一个 F_ϕ- 同构 π. 显然 π 是 R_1 到 L 的一个嵌入.

将 K 的正规位 ϕ_B 和 π 合成, 即得到 K 到 L 的一个位 ψ. 易见, ψ 是位 ϕ 在 K 上的一个拓展.

现设 ψ 是 K 的一个 L- 值位, 且 ψ 是 ϕ 的一个拓展. 由定理 3.3.3 的推论知, K 有一个序 $\leqslant$, 使得 ψ 与 $\leqslant$ 相容. 此时易知, ϕ 与 $\leqslant$ 在 F 上的限制相容. 证毕.

作为定理 3.3.5 的一个应用, 可建立如下结论.

定理 3.3.6 设 ϕ 是域 F 的一个 L- 值位, 其中 L 是一个实闭域, 且 $\leqslant$ 是 F 的一个序, 则 ϕ 与 $\leqslant$ 相容, 当且仅当 ϕ 可以惟一地拓展为 R 的一个 L- 值位, 这里 R 表示序域 $(F, \leqslant)$ 的实闭包.

证明 设 ϕ 可以惟一地拓展为 R 的一个 L- 值位 ψ. 由定理 3.3.3 的推论知, ψ 与 R 的惟一序 $\leqslant_{R^2}$ 相容. 此时易知, ϕ 与 $\leqslant$ 相容.

反过来, 设 ϕ 与 $\leqslant$ 相容. 由定理 3.3.5 知, ϕ 可以拓展为 R 的一个 L- 值位 ψ. 设 A_ϕ 和 B_ψ 分别为 ϕ 和 ψ 的赋值环. 根据命题 3.3.2, $A_\phi = A(E, \leqslant)$, 其中 E 是 F 的一个子域. 由定理 3.2.5 中的惟一性知, $B_\psi = A(E, \leqslant_{R^2})$, 这里 $\leqslant_{R^2}$ 为 R 的惟一序. 这表明 ψ 实际上等价于 R 的关于子域 E 和序 $\leqslant_{R^2}$ 的典型实位. 证毕.

对于 $\mathbb{R}$- 值位的拓展，上面有关定理可进一步改进如下.

定理 3.3.7 设 ϕ 是域 F 的一个 $\mathbb{R}$- 值位， K 是 F 的一个扩张，则 ϕ 可以拓展为 K 的一个 $\mathbb{R}$- 值位，当且仅当 K 有一个序 $\leqslant$, 使得 ϕ 与 $\leqslant$ 在 F 上的限制相容.

证明 必要性的证明类似于定理 3.3.5, 下证充分性.

设 K 有一个序 $\leqslant$, 使得 ϕ 与 $\leqslant_F$ 相容，其中 $\leqslant_F$ 表示 $\leqslant$ 在 F 上的限制. 令 A_ϕ 是 ϕ 的赋值环，则由命题 3.3.2 知， $A_\phi = A(E, \leqslant_F)$, 其中 E 是 F 的一个子域. 注意到 $\mathbb{Q} \subseteq E$, 从而 $A(\mathbb{Q}, \leqslant_F) \subseteq A(E, \leqslant_F)$. 设 $a \in A_\phi$, 则 $\phi(a) \in \mathbb{R}$. 由于 $\mathbb{R}$ 的惟一序 $\leqslant_{\mathbb{R}^2}$ 是阿基米德序，从而有 $q \in \mathbb{Q}$, 使得 $|\phi(a)| <_{\mathbb{R}^2} q$, 即 $-q <_{\mathbb{R}^2} \phi(a) <_{\mathbb{R}^2} q$. 由 ϕ 与序 $\leqslant_F$ 的相容性知， $-q <_F a <_F q$. 由此可见， $a \in A(\mathbb{Q}, \leqslant_F)$. 因而 $A_\phi = A(\mathbb{Q}, \leqslant_F)$. 令 ψ 是 K 的关于 $\leqslant$ 的典型 $\mathbb{R}$- 值位，则 ψ 的赋值环为 $A(\mathbb{Q}, \leqslant)$. 显然 $A(\mathbb{Q}, \leqslant) \cap F = A(\mathbb{Q}, \leqslant_F)$, 因此 ψ 是位 ϕ 在 K 上的一个拓展. 证毕.

根据定理 3.3.7 的证明，可附带地获得下面结果.

命题 3.3.8 设 ϕ 是域 F 的一个 $\mathbb{R}$- 值位，则对于 F 的每个与 ϕ 相容的序 $\leqslant$, 都有 $A_\phi = A(\mathbb{Q}, \leqslant)$, 这里 A_ϕ 是 ϕ 的赋值环.

§3.4 实 Hensel 赋值

Hensel 赋值是一类重要赋值. 在本节中，实 Hensel 赋值将得到研究. 域 F 的一个赋值 v 称作 Hensel 赋值，如果 v 在 F 的每个代数扩张上有惟一拓展，这里的 "惟一性" 是指赋值等价的意义下的惟一性. 此时， v 的赋值环 A_v 称作域 F 的一个 Hensel 赋值环. 显然，域 F 的一个赋值 v 是 Hensel 赋值，当且仅当 v 在 F 的代数闭包上有惟一拓展. 设 v 是域 F 的任意一个赋值， K 是 F 的一个扩张， w 是赋值 v 在 K 上一个拓展. 如果 v 和 w 的值群相同，且剩余域 A_v/M_v 到 A_w/M_w 的自然嵌入是一个同构，那么称 w 是 v 的一个直接扩张，或称 (K, w) 是赋值域 (F, v) 的一个直接扩张.

下面结论是赋值论中关于 Hensel 赋值的熟知事实，这些事实对于本节的讨论是必需的.

命题 3.4.1 (1) 域 F 的一个赋值 v 是 Hensel 赋值，当且仅当下面两个条件之一成立:

(i)v 的赋值环 A_v 满足如下 Hensel 引理：对于多项式 $f(x) \in A_v[x]$, 若有 $F_v[x]$ 中两个互素多项式 $\phi(x)$ 和 $\psi(x)$, 使得 $\bar{f}(x) = \phi(x)\psi(x)$, 其中 $\bar{f}(x)$ 表示 $f(x)$ 在自然同态: $A_v[x] \longrightarrow A_v/M_v[x]$ 下的象，则有 $g(x), h(x) \in A_v[x]$, 使得 $f(x) = g(x)h(x)$, $\bar{g}(x) = \phi(x)$, $\bar{h}(x) = \psi(x)$, 且 $g(x)$ 和 $\phi(x)$ 具有相同的次数.

(ii) 对于首项系数为 1 的多项式 $f(x) \in A_v[x]$, 若 $f(x)$ 在自然同态: $A_v[x] \longrightarrow$

$A_v/M_v[x]$ 下的象 $\bar{f}(x)$ 在剩余域 A_v/M_v 中有单根 β, 则有 $b \in A_v$, 使得 $f(b)=0$, 且 $\beta = \bar{b} := b + M_v$.

(2) 若域 F 的一个赋值 v 在 F 的每个真代数扩张上的拓展都不是直接扩张，则 v 是 F 的一个 Hensel 赋值.

(3) 每一个赋值域 (F, v) 都有这样的 Hensel 代数扩张 (K, w), 使得对于 F 和 K 的每个不等于 K 的中间域 E, w 在 E 上的限制 $w\,|_E$ 不再是 Hensel 赋值.

上面命题的叙述 (3) 中，满足所述条件的 Hensel 代数扩张 (K, w) 称作赋值域 (F, v) 的一个 Hensel 化. 对于赋值域 (F, v) 的 Hensel 化，有下列熟知的结果.

命题 3.4.2 (1) 赋值域 (F, v) 的每个 Hensel 扩张都包含 (F, v) 的一个 Hensel 化.

(2) 赋值域 (F, v) 的每个 Hensel 化都是直接扩张.

(3) 若 (K_1, w_1) 和 (K_2, w_2) 都是赋值域 (F, v) 的 Hensel 化，则存在 K_1 到 K_2 的一个 F- 同构 π, 使得对于每个 $a \in K_1$, $w_1(a) = w_2(\pi(a))$.

定义 3.4.1 域 F 上一个赋值 v 称作实 Hensel 赋值，如果 v 是实赋值，同时也是 Hensel 赋值.

命题 3.4.3 实闭域的每个实赋值都是 Hensel 赋值.

证明 设 R 是一个实闭域，v 是 R 的一个实赋值，且 A, M 分别是 v 的赋值环和赋值理想.

设 $f(x) \in A[x]$ 是一个首项系数为 1 的多项式，且 $\bar{f}(x) = u(x)v(x)$, 其中 $u(x)$, $v(x)$ 是 $A/M[x]$ 中的两个互素的首项系数为 1 的多项式. 由定理 2.1.3 的推论知，$f(x)$ 在 $R[x]$ 可分解如下:

$$f(x) = (x-a_1)\cdots(x-a_m)[(x-b_1)^2+c_1^2]\cdots[(x-b_n)^2+c_n^2],$$

其中 $a_i, b_j, c_j \in R$, 且 $c_j \neq 0$, $i=1,\cdots,m$; $j=1,\cdots,n$.

显然，a_i, $b_j + c_j\sqrt{-1}$ 和 $b_j - c_j\sqrt{-1}$ 在环 A 上整，$i=1,\cdots,m$; $j=1,\cdots,n$. 于是 $b_j^2+c_j^2 = (b_j+c_j\sqrt{-1})(b_j-c_j\sqrt{-1})$ 在环 A 上整，$j=1,\cdots,n$. 由于赋值环 A 在 R 中是整闭的，从而有 $a_i \in A$, $i=1,\cdots,m$, 且 $b_j^2+c_j^2 \in A$, $j=1,\cdots,n$. 由于 v 是一个实赋值，从而由命题 3.1.2 的推论 1 知，$b_j, c_j \in A$, $j=1,\cdots,n$.

由上面分解式有

$$\bar{f}(x) = (x-\bar{a}_1)\cdots(x-\bar{a}_m)[(x-\bar{b}_1)^2+\bar{c}_1^2]\cdots[(x-\bar{b}_n)^2+\bar{c}_n^2],$$

其中 $\bar{z} := z + M$, 对于每个 $z \in A$.

由此有 $(x-\bar{a}_i)|u(x)v(x)$, 进而有 $(x-\bar{a}_i)|u(x)$ 或者 $(x-\bar{a}_i)|v(x)$, $i=1,\cdots,m$. 同样有 $(x-\bar{b}_j)^2+\bar{c}_j^2|u(x)v(x)$, $j=1,\cdots,n$. 当 $\bar{c}_j \neq 0$ 时，$(x-\bar{b}_j)^2+\bar{c}_j^2$ 在 $A/M[x]$ 中也是不可约的，因为 A/M 是一个实域. 此时必有，$(x-\bar{b}_j)^2+\bar{c}_j^2|u(x)$

或 $(x-\bar{b}_j)^2+\bar{c}_j^2|v(x)$. 当 $\bar{c}_j=0$ 时, $(x-\bar{b}_j)^2|u(x)v(x)$. 由于 $u(x)$ 和 $v(x)$ 互素, 从而仍有 $(x-\bar{b}_j)^2|u(x)$ 或 $(x-\bar{b}_j)^2|v(x)$. 因而总有, $(x-\bar{b}_j)^2+\bar{c}_j^2|u(x)$ 或 $(x-\bar{b}_j)^2+\bar{c}_j^2|v(x)$, $j=1,\cdots,n$.

由上面讨论, 可设 $x-\bar{a}_1,\cdots,x-\bar{a}_r$, $(x-\bar{b}_1)^2+\bar{c}_1^2,\cdots,(x-\bar{b}_s)^2+c_s^2$ 是 $u(x)$ 的因式, 而 $x-\bar{a}_{r+1},\cdots,x-\bar{a}_m$, $(x-\bar{b}_{s+1})^2+\bar{c}_{s+1}^2,\cdots,(x-\bar{b}_n)^2+c_n^2$ 是 $v(x)$ 的因式. 令 $g(x)=(x-a_1)\cdots(x-a_r)[(x-b_1)^2+c_1^2]\cdots[(x-b_s)^2+c_s^2]$, 而 $h(x)=(x-a_{r+1})\cdots(x-a_m)[(x-b_{s+1})^2+c_{s+1}^2]\cdots[(x-b_n)^2+c_n^2]$. 易见, $f(x)=g(x)h(x)$, 且 $\bar{g}(x)=u(x)$, $\bar{h}(x)=v(x)$. 由命题 3.4.1(1) 知, v 是一个 Hensel 赋值. 证毕.

定理 3.4.4 设 v 是域 F 的一个实赋值, 则对于赋值域 (F,v) 的每个 Hensel 化 (K,w), w 是 K 的一个实赋值.

证明 由命题 3.4.2(2) 知, (K,w) 是 (F,v) 的直接扩张. 因而, $F_w\cong F_v$, 这里 F_v 和 F_w 分别为 v 和 w 的剩余域. 由所设知, F_v 是一个实域. 从而 F_w 也是一个实域, 即 w 是 K 的一个实赋值. 证毕.

下面定理反映出 Hensel 赋值和序之间的重要关系.

定理 3.4.5 设 (F,v) 是一个 Hensel 赋值域, 则对于 F 的每个序 $\leqslant$, v 与 $\leqslant$ 相容.

证明 设 A 和 M 分别为 v 的赋值环和赋值理想. 对于每个 $b\in M$, $f(x)=x^2+x+b\in A[x]$, 且在 $A/M[x]$ 中有分解式 $\bar{f}(x)=x(x+1)$, 其中 x, $x+1$ 是 $A/M[x]$ 中互素的多项式. 由 Hensel 条件知, $f(x)=(x-a)(x-c)$, 其中 $a,c\in A$. 注意到 F 的特征为零. 由此有 $1-b=1+(a^2+a)=(a+\frac{1}{2})^2+\frac{3}{4}>0$. 因而有 $b<1$. 由命题 3.1.3 知, v 与序 $\leqslant$ 相容. 证毕.

推论 设 v 是域 F 的一个 Hensel 赋值, 则 v 是实赋值, 当且仅当 F 是实域.

证明 由命题 3.1.2 的推论 2 知, 必要性成立. 现设 F 是一个实域, 则由定理 1.1.3 知, F 至少有一个序 $\leqslant$. 由定理 3.4.5 知, v 与 $\leqslant$ 相容. 根据定理 3.1.4, v 是一个实赋值. 证毕.

上面推论表明, 实域的每个 Hensel 赋值都是实 Hensel 赋值.

引理 3.4.6 设 v 是域 F 的一个实赋值, K 是域 F 的一个扩张, w 是赋值 v 在 K 上的一个直接扩张, 则从 $\mathcal{X}_K^w$ 到 $\mathcal{X}_F^v$ 的限制映射 r: $Q\longmapsto Q\cap F$ 是一个同胚映射.

证明 由条件知, v 和 w 的剩余域是自然同构的, 从而 w 是 K 的一个实赋值. 根据命题 3.2.6, 限制映射 r 是一个连续映射. 注意到 $\mathcal{X}_K^w$ 和 $\mathcal{X}_F^v$ 均为 Hausdorff 的紧空间. 由拓扑学知识知, 只须再证明 r 是一一对应.

对于 $P\in\mathcal{X}_F^v$, 构造 K 的如下子集:

$$T = \left\{ \sum_{i=1}^{n} p_i \alpha_i^2 (1-\eta_i) \mid p_i \in P, \alpha_i \in K, \eta_i \in M_w, i = 1, \cdots, n \right\}.$$

易见，$P \cup K^2 \subseteq T, T+T \subseteq T$，且 $T \cdot T \subseteq T$. 假若 $-1 \in T$，则 $-1 = \sum_{i=1}^{n} p_i \alpha_i^2 (1-\eta_i)$，其中 $p_i \in P$, $\alpha_i \in K$, $\eta_i \in M_w$，且 p_i 和 α_i 均非零，$i = 1, \cdots, n$. 由于 w 和 v 的值群相同，从而有 $a_i \in F$，使得 $w(\alpha_i) = v(a_i) = w(a_i)$, $i = 1, \cdots, n$. 令 $\beta_i = \alpha_i a_i^{-1}$，则 $\beta_i \in A_w$，但 $\beta_i \notin M_w$. 又由于 A_v/M_v 和 A_w/M_w 是自然同构的，从而有 $b_i \in A_v$，使得 $\beta_i + M_w = b_i + M_w$, $i = 1, \cdots, n$. 于是有 $\xi_i \in M_w$，使得 $\beta_i = b_i + \xi_i$, $i = 1, \cdots, n$. 由上面的等式有，$1 + \sum_{i=1}^{n} r_i (b_i + \xi_i)^2 (1-\eta_i) = 0$，其中 $r_i = p_i a_i^2 \in P$, $i = 1, \cdots, n$. 记 $r_0 = b_0 = 1 \in P$，且令 $v(r_k) = \min\{v(r_i) \mid i = 0, 1, \cdots, n\}$, $0 \leqslant k \leqslant n$, $q_i = r_i r_k^{-1}$, $i = 0, \cdots, n$，则 $q_i \in A_v \cap P$, $i = 0, 1, \cdots, n$. 从而 $q_0 + \sum_{i=1}^{n} q_i (b_i + \xi_i)^2 (1-\eta_i) = 0$，即有 $q_0 b_0^2 + \sum_{i=1}^{n} q_i b_i^2 = \sum_{i=1}^{n} q_i [b_i^2 - (b_i + \xi_i)^2 (1-\eta_i)] \in M_w \cap F = M_v$. 此时有 $0 \leqslant_P b_k^2 = q_k b_k^2 \leqslant_P q_0 b_0^2 + \sum_{i=1}^{n} q_i b_i^2$. 由于 M_v 关于 $\leqslant_P$ 是凸的，从而 $b_k^2 \in M_v$ 即 $b_k \in M_v$，矛盾. 因而，T 是域 K 的一个亚正锥. 由定理 1.1.2 的推论，K 有一个正锥 Q，使得 $T \subseteq Q$. 注意到 $1 + M_w \subseteq Q$，从而由命题 3.1.3 知，$Q \in \mathcal{X}_K^w$. 显然，$P \subseteq Q \cap F$. 从而必有 $Q \cap F = P$. 因而 r 是一个满射.

设 $Q_1, Q_2 \in \mathcal{X}_K^w$，使得 $Q_1 \cap F = Q_2 \cap F$. 假若 $Q_1 \neq Q_2$，则有非零 $\alpha \in K$，使得 $\alpha \in Q_1$，但 $-\alpha \in Q_2$. 由于 (K, w) 是 (F, v) 的直接扩张，从而有 $a \in F$，使得 $w(\alpha) = v(a) = w(a)$. 由于 $w(a) = w(-a)$，从而不妨设 $a \in Q_1$. 于是 $a \in Q_1 \cap F = Q_2 \cap F$. 令 $\beta = \alpha a^{-1}$，则 $w(\beta) = 0$, $\beta \in Q_1$，但 $-\beta \in Q_2$. 记 $\overline{Q}_1$ 和 $\overline{Q}_2$ 是在剩余域 F_w 上分别由 Q_1 和 Q_2 所诱导的正锥，则 $\beta + M_w \in \overline{Q}_1$，但 $-\beta + M_w \in \overline{Q}_2$. 注意到 A_v/M_v 和 A_w/M_w 是自然同构的. 从而有 $b \in A_v$，使得 $\beta + M_w = b + M_w$. 于是 $b + M_w \in \overline{Q}_1$，但 $-b + M_w \in \overline{Q}_2$. 由命题 3.1.3 的推论后面的事实可知，$b \in Q_1$，但 $-b \in Q_2$. 此时有 $b \in Q_1 \cap F = Q_2 \cap F \subseteq Q_2$. 从而 $b \in Q_2 \cap -Q_2$，即 $b = 0$，矛盾. 因此，r 是一个单射. 证毕.

定理 3.4.7 设 (K, w) 是赋值域 (F, v) 的一个 Hensel 化，$\leqslant$ 是 F 的一个序，则 v 与 $\leqslant$ 相容，当且仅当 $\leqslant$ 可以拓展为 K 的一个序. 此时，序 $\leqslant$ 在 K 上的拓展是惟一的.

证明 设 $\leqslant$ 可以拓展为 K 的一个序 $\leqslant_K$，则由定理 3.4.4, w 与 $\leqslant_K$ 相容. 由此可知，v 与 $\leqslant$ 相容.

现设 v 与 $\leqslant$ 相容，且令 P 为序 $\leqslant$ 的对应正锥，则 $P \in \mathcal{X}_F^v$. 根据命题 3.4.2(2),

(K,w) 是 (F,v) 的一个直接扩张. 由引理 3.4.6 知, 从 $\mathcal{X}_K^w$ 到 $\mathcal{X}_F^v$ 的限制映射 r 是一个同胚映射. 从而, 正锥 P 在 K 上有惟一的拓展 Q. 因而序 $\leqslant$ 在 K 上有惟一的拓展 $\leqslant_Q$, 这里 $\leqslant_Q$ 是 Q 的对应序. 证毕.

推论 设 (K,w) 是赋值域 (F,v) 的一个 Hensel 化, 且 v 是 F 的一个实赋值, 则 w 是赋值 v 在 K 上惟一的实拓展.

证明 设 w_1 是 v 在 K 上的任意实拓展. 由定理 3.1.4 知, w_1 与 K 的一个序 $\leqslant$ 相容. 再由定理 3.4.5 知, w 也与 $\leqslant$ 相容. 设 R 是序域 $(K,\leqslant)$ 的实闭包. 由定理 3.2.5 知, w 和 w_1 都可分别惟一地拓展为 R 的实赋值 u 和 u_1. 记 $\leqslant_F$ 是序 $\leqslant$ 在 F 上的限制. 由于 w_1 与 $\leqslant$ 相容, 从而显然 v 与 $\leqslant_F$ 相容. 注意到, K 是 F 的代数扩张, 从而 R 也是序域 $(F,\leqslant_F)$ 的实闭包. 由定理 3.2.5 中的惟一性知, u 和 u_1 具有相同的赋值环, 从而 w 和 w_1 具有相同的赋值环. 因此, 在赋值等价的意义下, $w_1=w$. 证毕.

作为实 Hensel 赋值的一个刻画, 可以建立如下定理.

定理 3.4.8 设 v 是域 F 的一个实赋值, 则 v 是 Hensel 赋值, 当且仅当对于赋值域 (F,v) 的每个有限扩张 (K,w), $\mathcal{X}_K=\mathcal{X}_K^w$.

证明 设 v 是域 F 的 Hensel 赋值, 则由定义易知, (F,v) 的每个有限扩张 (K,w) 也是 Hensel 的. 根据定理 3.4.5 可知, $\mathcal{X}_K=\mathcal{X}_K^w$.

现设对于 (F,v) 的每个有限扩张 (K,w), $\mathcal{X}_K=\mathcal{X}_K^w$, 则易知, 对于 (F,v) 的每个代数扩张 (K,w), $\mathcal{X}_K=\mathcal{X}_K^w$. 由定理 3.1.4 知, F 有一个正锥 P, 使得 v 与 P 相容. 记 R 为序域 (F,P) 的实闭包, 且令 w 是 v 在 R 上的任意拓展, 则 $\mathcal{X}_R^w=\mathcal{X}_R=\{R^2\}$. 这表明 w 与 R^2 相容, 即 w 是 v 在 R 上的实拓展. 由定理 3.2.5 知, w 是 v 在 R 上的惟一拓展. 此外, 由命题 3.4.3 知, w 是 R 的 Hensel 赋值. 从而, 赋值 w 在 $R(\sqrt{-1})$ 上仅有惟一拓展. 这样, v 在 F 的代数闭包 $R(\sqrt{-1})$ 上仅有惟一拓展. 根据定义易知, v 是 F 的 Hensel 赋值. 证毕.

引理 3.4.9 设 v 是实闭域 R 的一个赋值, 则 v 的剩余域 F_v 是实闭的或代数闭的.

证明 由赋值的拓展定理知, v 可拓展为 $R(\sqrt{-1})$ 上的一个赋值 w. 设 F_w 是 w 的剩余域. 由于 $R(\sqrt{-1})$ 是代数闭域, 从而 F_w 也是代数闭域. 由赋值论知识, $[F_w:F_v]\leqslant[R(\sqrt{-1}):R]=2$. 当 $[F_w:F_v]=1$ 时, $F_v=F_w$ 是代数闭域; 当 $[F_w:F_v]=2$ 时, 由定理 2.1.5 知, F_v 是一个实闭域.

作为实闭域在赋值理论方面的一个刻画, 可建立下面结论.

定理 3.4.10 设 v 是域 F 的一个实赋值, 则 F 是实闭域, 当且仅当如下三个条件都成立:

(1) v 的值群 G_v 是一个可除群, 即对于任意 $g\in G_v$ 以及任意自然数 n, 有 $h\in G_v$, 使得 $g=nh$.

(2) 剩余域 F_v 是实闭域.

(3) v 是 F 的 Hensel 赋值.

证明 设 F 是一个实闭域. 由命题 3.4.3 知, v 是 F 的一个 Hensel 赋值. 注意到 F_v 是实域, 从而由引理 3.4.9 知, F_v 是实闭域. 对于任意 $g \in G_v$, 有 $a \in F$, 使得 $v(a) = g$. 注意到 $v(a) = v(-a)$, 从而可设 $0 < a$, 这里 $\leqslant$ 为 F 的惟一序. 由中间值定理可知, 多项式 $x^n - a$ 在 F 中有一个根 b, 这里 n 是任意自然数. 于是 $g = v(a) = v(b^n) = nv(b)$, 其中 $v(b) \in G_v$. 因而, G_v 是一个可除群.

现设条件 (1), (2) 和 (3) 都成立. 由定理 3.1.4 知, F 有一个序 $\leqslant$, 使得 v 与 $\leqslant$ 相容. 设 R 是序域 $(F, \leqslant)$ 的实闭包, 则由定理 3.2.5 知, v 可以拓展为 R 的一个实赋值 w. 令 G_w 和 F_w 分别为 w 的值群和剩余域, 则 G_v 和 F_v 分别是 G_w 和 F_w 的子群和子域. 由于商群 G_w/G_v 中每个元素的阶是有限的, 且 G_v 是可除群, 从而必有 $G_w = G_v$. 此外, 由于 F_w 是 F_v 的实代数扩张, 且 F_v 是实闭域, 从而 $F_w = F_v$.

假若 $F \neq R$, 则有 $\alpha \in R$, 使得 $\alpha \notin F$. 设 α 在 F 上的极小多项式为 $x^n + a_1x^{n-1} + \cdots + a_n$, 其中 $a_1, \cdots, a_n \in F$, 且 $n > 1$. 令 $\beta = \alpha + \frac{1}{n}a_1$, 则 β 在 F 上的极小多项式具有形式 $x^n + b_2x^{n-2} + \cdots + b_n$, 其中 $b_2, \cdots, b_n \in F$. 由于 $G_w = G_v$, 从而有 $e \in F$, 使得 $w(\beta) = v(e) = w(e)$. 再令 $\gamma = \beta e^{-1}$, 则 $w(\gamma) = 0$, 且 γ 在 F 上的极小多项式具有这样的形式: $f(x) = x^n + c_2x^{n-2} + \cdots + c_n$, 其中 $c_2, \cdots, c_n \in F$. 令 A_v 和 A_w 分别是 v 和 w 的赋值环. 由于 v 是 Hensel 赋值, 从而 A_w 是 A_v 在 R 中的惟一拓展. 因而 A_w 实际上是 A_v 在 R 中的整闭包, 从而 $\gamma \in A_w$ 在 A_v 上整. 于是 $f(x) \in A_v[x]$. 由于 $F_w = F_v$, 从而有 $d \in A_v$, 使得 $\gamma + M_w = d + M_w$, 这里 M_w 是 w 的赋值理想. 由此有 $f(d) = f(d) - f(\gamma) \in M_w$, 即有 $f(d) \in M_w \cap F = M_v$, 这里 M_v 是 v 的赋值理想. 设 $\bar{f}(x)$ 是 $f(x)$ 在 $F_v[x] = A_v/M_v[x]$ 中的对应多项式, 则 $\bar{f}(\bar{d}) = 0$, 这里 $\bar{d} = d + M_v \in F_v$. 从而在 $F_v[x]$ 中, $x - \bar{d} | \bar{f}(x)$. 如若 $x - \bar{d}$ 是 $\bar{f}(x)$ 的惟一的 (首项系数为 1 的) 不可约因式, 则 $\bar{f}(x) = (x - \bar{d})^n$. 注意到 $\bar{f}(x)$ 中项 x^{n-1} 的系数为零, 从而 $n\bar{d} = 0$. 由于 F_v 的特征为零, 从而 $\bar{d} = 0$, 即 $d \in M_v \subseteq M_w$. 于是 $\gamma \in M_w$, 矛盾. 如若 $\bar{f}(x)$ 除 $x - \bar{d}$ 外还有其他的首项系数为 1 的不可约因式, 则 $\bar{f}(x)$ 可表示为 $\bar{f}(x) = \phi(x)\psi(x)$, 其中 $\phi(x)$ 和 $\psi(x)$ 是 $F_v[x]$ 中两个互素的多项式, 且 $0 < \deg\phi(x) < n$. 根据 Hensel 条件可知, $f(x)$ 在 $A_v[x]$ 中可约, 矛盾. 因此, $F = R$, 即 F 是一个实闭域. 证毕.

§3.5 实 全 纯 环

本节将考虑域中与实赋值相关的一类子环 —— 实全纯环, 从而得到这类子环的结构. 此外, 我们研究域的实赋值环与实全纯环的素理想之间的对应关系.

设 (F, T) 是一个亚序域, $\mathcal{X}_F(T)$ 是它的序空间, 且 D 是 F 的一个包含单位

元 1 的子环.

定义 3.5.1 所设同上，域 F 的所有与 T 相容且包含子环 D 的 (实) 赋值环之交集称作 F 关于亚序 T 和子环 D 的实全纯环，且记作 $H_F(T,D)$. 特别地，当 $D=\mathbb{Q}$ 时，相应的实全纯环径称作 (F,T) 的实全纯环，且简记为 $H_F(T)$; 当 $T=\sum F^2$ 且 $D=\mathbb{Q}$ 时，相应的实全纯环径称作 F 的实全纯环，且简记为 H_F.

显然，实全纯环 H_F 是 F 的全体实赋值环的交集. 而 $H_F(T)$ 是 F 的所有与 T 相容的赋值环的交集.

对于 $P\in\mathcal{X}_F(T)$, 按照 §3.1, 可得到子环 D 关于序 $\leqslant_P$ 的凸包 $C(D,\leqslant_P)$. 为简便起见，记 $C(D,P)$ 为这样一个凸包. 注意到 $\mathbb{Z}\subseteq D$, 从而有 $A(\mathbb{Q},\leqslant_P)=C(\mathbb{Z},P)\subseteq C(D,P)$. 由于 $A(\mathbb{Q},\leqslant_P)$ 是 F 的一个 (实) 赋值环，从而 $C(D,P)$ 也是 F 的一个赋值环. 根据命题 3.1.3 和定理 3.1.5 可知， $C(D,P)$ 是一个与 T 相容的实赋值环.

设 A 是 F 的任意一个与 T 相容且包含 D 的实赋值环. 根据定理 3.1.5 知，对于某个 $P\in\mathcal{X}_F(T)$, A 的赋值与 P 相容. 再由命题 3.1.3 知， A 关于 $\leqslant_P$ 是凸的. 从而易见， $C(D,P)\subseteq A$.

由上面讨论，下面命题成立.

命题 3.5.1 所设同上，则

$$H_F(T,D)=\bigcap_{P\in\mathcal{X}_F(T)}C(D,P).$$

由上面命题可见，我们可以把关于实全纯环 $H_F(T,D)$ 的结构问题转化为讨论交集 $\bigcap_{P\in\mathcal{X}_F(T)}C(D,P)$ 中元素的形式.

定理 3.5.2 设 (F,T) 是一个亚序域， D 是 F 的一个子环，则对于 $x\in F$, 下列叙述等价:

(1) $x\in\bigcap_{P\in\mathcal{X}_F(T)}C(D,P)$;

(2) 对于某个 $d\in D$, $d\pm x\in T$.

证明 (1) $\Longrightarrow$ (2): 对于每个 $P\in\mathcal{X}_F(T)$, 由叙述 (1) 有 $x\in C(D,P)$. 由 $C(D,P)$ 的结构知，有 $d_P\in D$, 使得 $-d_P\leqslant_P x\leqslant_P d_P$, 即 $d_P\pm x\in P$. 这表明: $P\in H(d_P+x,d_P-x)$. 因而有 $\mathcal{X}_F(T)\subseteq\bigcup_{P\in\mathcal{X}_F(T)}H(d_P+x,d_P-x)$. 由定理 1.5.4 知，关于 $\mathcal{X}_F$ 的 Harrison 拓扑， $\mathcal{X}_F(T)$ 是 $\mathcal{X}_F$ 的一个紧子集. 从而存在有限个 $P_1,\cdots,P_n\in\mathcal{X}_F(T)$, 使得 $\mathcal{X}_F(T)\subseteq\bigcup_{i=1}^{n}H(d_{P_i}+x,d_{P_i}-x)$. 令 $d=\frac{1}{4}+d_{P_1}^2+\cdots+d_{P_n}^2$. 对于每个 $P\in\mathcal{X}_F(T)$, 有某个 $j\in\{1,\cdots,n\}$, 使得 $P\in H(d_{P_j}+x,d_{P_j}-x)$, 即 $d_{P_j}\pm x\in P$. 此时， $d\pm x=(d_{P_j}\pm x)+(d_{P_j}-\frac{1}{2})^2+\sum_{i\neq j}d_{P_i}^2\in P$. 由定理 1.1.2 知， $d\pm x\in T$.

(2) $\Longrightarrow$ (1): 对于每个 $P \in \mathcal{X}_F(T)$, $d \pm x \in T \subseteq P$, 即 $-d \leqslant_P x \leqslant_P d$. 从而 $x \in C(D,P)$. 证毕.

现在可以建立下面的主要定理, 这一定理给出了实全纯环 $H_F(T,D)$ 中元素的形式.

定理 3.5.3 设 (F,T) 是一个亚序域, D 是 F 的子环, 则对于 $x \in F$, 下列叙述等价:

(1) $x \in H_F(T,D)$;

(2) 对于某个 $t \in T$, $x^2 + t \in D$;

(3) $x \in D[(1+t)^{-1} \mid t \in T]$, 这里 $D[(1+t)^{-1} \mid t \in T]$ 表示将子集 $\{(1+t)^{-1} \mid t \in T\}$ 添加到子环 D 上所得到的扩环.

证明 (1) $\Longleftrightarrow$ (2): 设 $x \in H_F(T,D)$, 则显然 $x^2 \in H_F(T,D)$. 根据命题 3.5.1, $x^2 \in \bigcap_{P \in \mathcal{X}_F(T)} C(D,P)$. 再由定理 3.5.2 知, 有 $d \in D$, 使得 $d - x^2 \in T$. 令 $t = d - x^2 \in T$, 则 $x^2 + t = d \in D$.

再设 A 是 F 的任意一个与 T 相容且包含 D 的赋值环. 由定理 3.1.5 知, 有某个 $P \in \mathcal{X}_F(T)$, 使得 A 的赋值与 P 相容, 即 A 关于序 $\leqslant_P$ 是凸的. 由叙述 (2) 知, $0 \leqslant_P x^2 \leqslant_P x^2 + t \in D \subseteq A$. 从而 $x^2 \in A$, 即 $x \in A$. 由 A 的任意性知, 叙述 (1) 成立.

(1) $\Longleftrightarrow$ (3): 设 $x \in H_F(T,D)$. 由命题 3.5.1 和定理 3.5.2 可知, 有 $d \in D$, 使得 $d \pm x \in T$. 令 $t_1 = d + x$, 且 $t_2 = d - x$, 则 $t_1, t_2 \in T$, 且 $(d+1+x)(1+t_2) = (1+t_1)(d+1-x)$. 由此可得 $x = (d+1)[(1+t_3)^{-1} - (1+t_4)^{-1}]$, 其中 $t_3 = (1+t_2)(1+t_1)^{-1}$, $t_4 = (1+t_1)(1+t_2)^{-1} \in T$. 从而, $x \in D[(1+t)^{-1} \mid t \in T]$.

反过来, 设 $x \in D[(1+t)^{-1} \mid t \in T]$. 对于 F 的任意一个与 T 相容且包含 D 的赋值环 A, 由定理 3.1.5 知, 有某个 $P \in \mathcal{X}_F(T)$, 使得 A 关于序 $\leqslant_P$ 是凸的. 对于每个 $t \in T$, 显然有 $0 \leqslant_P (1+t)^{-1} \leqslant_P 1 \in A$. 从而 $(1+t)^{-1} \in A$. 因而 A 包含子集 $\{(1+t)^{-1} \mid t \in T\}$, 从而 $D[(1+t)^{-1} \mid t \in T] \subseteq A$. 于是 $x \in A$. 由 A 的任意性知, $x \in H_F(T,D)$. 证毕.

推论 1 设 (F,T) 是一个亚序域, 则 $H_F(T) = \mathbb{Q}[(1+t)^{-1} \mid t \in T]$.

推论 2 设 F 是一个实域, 则 $H_F = \mathbb{Q}[(1+t)^{-1} \mid t \in \sum F^2]$.

此外, 由定理 3.5.3, 容易建立下面结论.

定理 3.5.4 所设同定理 3.5.3, 则

$$H_F(T,D) = \{dx(1+x^2+t)^{-1} \mid d \in D, t \in T \text{ 且 } x \in F\}.$$

证明 设 $x \in H_F(T,D)$, 则由定理 3.5.3 中蕴含关系 "(1) $\Longrightarrow$ (2)" 知, 有 $t \in T$, 使得 $x^2 + t \in D$. 令 $d = 1 + x^2 + t \in D$, 则有 $x = dx(1+x^2+t)^{-1}$.

反过来，设 $y = dx(1+x^2+t)^{-1}$, 其中 $d \in D, t \in T$, 且 $x \in F$. 令 A 是 F 的任意一个与 T 相容且包含 D 的赋值环，则对于某个 $P \in \mathcal{X}_F(T)$, A 关于序 $\leqslant_P$ 是凸的. 此时，显然有 $0 \leqslant_P y^2 \leqslant_P d^2 \in D \subseteq A$. 从而 $y^2 \in A$, 即 $y \in A$. 由 A 的任意性， $y \in H_F(T, D)$. 证毕.

推论 设 (F, T) 是一个亚序域，则

$$H_F(T) = \{nx(1+x^2+t)^{-1} \mid n \in \mathbb{N}, t \in T \text{ 且 } x \in F\}.$$

现在，着手考虑实全纯环的素理想以及关于这些素理想的局部化. 为此，先证明如下引理:

引理 3.5.5 所设同定理 3.5.3, 则 F 的每个包含 $H_F(T, D)$ 的赋值环都与 T 相容.

证明 假若不然，则 F 有一个赋值环 A, 使得 $H_F(T, D) \subseteq A$, 但 A 不与 T 相容. 设 M 是 A 的极大理想. 由定理 3.1.5 的推论，剩余域 A/M 的子集 $\overline{T} := \{\bar{a} = a + M \mid a \in T \cap A\}$ 不是 A/M 的亚正锥. 这表明： $-1 \in \overline{T}$, 即对于某个 $t \in T \cap A$, $-1 = \bar{t}$. 从而 $1 + t \in M$. 由定理 3.5.3 知， $(1+t)^{-1} \in H_F(T, D) \subseteq A$. 由此有，$1 = (1+t)^{-1}(1+t) \in M$, 矛盾. 引理获证.

引理 3.5.6(Dress 引理) 设 F 是一个特征不等于 2 的域， B 是 F 的一个子环，使得对于每个 $y \in F$, $(1+y^2)^{-1} \in B$, 只要 $1 + y^2 \neq 0$, 则对于 B 的每个素理想 $\wp$, B 关于 $\wp$ 的局部化 $B_\wp$ 为 F 的赋值环. 特别地， F 是 B 的分式域.

证明 由条件知， $B_\wp$ 是 F 的一个包含 B 的局部子环，且对于每个 $y \in F$, $(1+y^2)^{-1} \in B_\wp$, 只要 $1 + y^2 \neq 0$. 因此，不妨直接设 B 是一个局部子环，由此只须证明 B 是 F 的一个赋值环. 设 M 是 B 的极大理想. 为此，我们证明如下两个断言.

断言 1 对于每个非零 $a \in F$, $a^2 \in B$ 或 $(a^{-1})^2 \in B$.

事实上，如若 $a^2 \notin B$, 则 $1 + a^2 \notin B$. 由于 $(1+a^2)^{-1} \in B$, 从而 $(1+a^2)^{-1} \in M$. 于是 $1 - (1+a^2)^{-1} \in B \setminus M$, 即 $a^2(1+a^2)^{-1} \in B \setminus M$. 由此有 $1 + (a^{-1})^2 = [a^2(1+a^2)^{-1}]^{-1} \in B$, 即有 $(a^{-1})^2 \in B$.

断言 2 若 $a^2 \in B$, 则 $a \in B$.

事实上，如若 $a \notin B$, 则 $2a \notin B$, 因为 $2 = 1 + 1^2$ 是 B 中可逆元. 从而 $(1+a)^2 = 1 + a^2 + 2a \notin B$. 由断言 1 知， $(1+a)^{-2} \in B$. 进而有 $(1+a)^{-2} \in M$. 因而 $(1+a^2)(1+a)^{-2} \in M$. 于是 $2a(1+a)^{-2} = 1 - (1+a^2)(1+a)^{-2} \in B \setminus M$. 由此有 $(1+a)^2(2a)^{-1} \in B$. 于是 $a = (2a^2) \cdot (1+a)^{-2} \cdot [(1+a)^2(2a)^{-1}] \in B$, 矛盾.

综合上面两个断言可知， B 是 F 的一个赋值环. 证毕.

定理 3.5.7 设 (F, T) 是一个亚序域，且 D 是 F 的一个子环，则 F 的所有与 T 相容且包含 D 的赋值环与实全纯环 $H_F(T, D)$ 的所有素理想之间存在一一对

应.

证明 为方便起见，简记 $H_F(T,D)$ 为 H, 记 $\mathcal{A}$ 为 F 的所有与 T 相容且包含 D 的赋值环组成的集合，且 $\mathcal{P}$ 为 H 的所有素理想组成的集合.

对于 $\wp\in\mathcal{P}$, 由引理 3.5.6 知， $H_\wp$ 是 F 的一个赋值环. 再由引理 3.5.5 知，$H_\wp$ 与 T 相容，即 $H_\wp\in\mathcal{A}$.

据此，可规定 $\mathcal{P}$ 到 $\mathcal{A}$ 的如下映射：

$$\phi:\ \wp\longmapsto H_\wp,\quad \wp\in\mathcal{P}.$$

设 $A\in\mathcal{A}$, 且 M 是 A 的极大理想. 令 $\wp=M\cap H$. 注意到 $H\subseteq A$, 从而 $\wp$ 是 H 的一个素理想，即 $\wp\in\mathcal{P}$. 显然 $H_\wp\subseteq A$. 假若 $A\neq H_\wp$, 则有 $a\in A$, 使得 $a\notin H_\wp$. 由于 $H_\wp$ 是 F 的一个赋值环，从而 a^{-1} 是 $H_\wp$ 中一个不可逆元素. 注意到 $H_\wp$ 的极大理想为 $\wp H_\wp$, 从而 $a^{-1}\in\wp H_\wp$, 即 $a^{-1}=bc^{-1}$, 其中 $b\in\wp$, $c\in H\setminus\wp$. 由于 $a\in A$ 且 $b\in\wp\subseteq M$, 从而有 $c=ab\in M$, 即有 $c\in M\cap H=\wp$, 矛盾. 因而， $A=H_\wp$. 这表明 ϕ 是一个满射.

设 $\wp_1,\wp_2\in\mathcal{P}$, 使得 $H_{\wp_1}=H_{\wp_2}$, 则 $H_{\wp_1}$ 和 $H_{\wp_2}$ 的极大理想相同，即 $\wp_1H_{\wp_1}=\wp_2H_{\wp_2}$. 由此有， $\wp_1=\wp_1H_{\wp_1}\cap H=\wp_2H_{\wp_2}\cap H=\wp_2$. 这表明 ϕ 是一个单射. 证毕.

推论 1 设 (F,T) 是一个亚序域，则 F 的所有与 T 相容的赋值环与实全纯环 $H_F(T)$ 的所有素理想之间存在一一对应.

推论 2 设 F 是一个实域，则 F 的所有实赋值环与实全纯环 H_F 的所有素理想之间存在一一对应.

§3.6 关于实函数域的 Lang 定理

域 F 上函数域实质上是域 F 的有限生成的超越扩张 $K=F(\alpha_1,\cdots,\alpha_m)$. 在代数几何中，域 F 上函数域是作为定义在 F 上的代数簇的函数域而出现的. 而在实代数几何中，域 F 上实函数域 可看作定义在 F 上的实簇的函数域.

关于函数域的实位的实质性系统研究是由 S. Lang 开始的. 在 Lang 的诸多成果中，有这样的三个特别重要定理：有理位的存在定理， Lang 同态定理和 Lang 嵌入定理. 尽管 Lang 同态定理可看作有理位的存在定理的一个推论，但它在解决 Hilbert 第十七问题中乃至实代数几何中有极其重要的作用.

设 $\phi: K\longrightarrow L\cup\{\infty\}$ 是域 K 的一个 L- 值. 如果 F 是 K 和 L 的共同子域，且 ϕ 在 F 上的限制是恒等嵌入 (即对于每个 $a\in F$, $\phi(a)=a$), 那么称 ϕ 是域 K 的一个 (L- 值) F- 位 . 如果同时又有： L 是 F 的一个代数扩张，那么称 ϕ 是一个代数 F- 位 . 若进一步有 $K=F$, 则称 ϕ 是一个有理 F- 位 .

引理 3.6.1 设 R 是一个实闭域， $R(x)$ 是 R 上的一元有理函数域， $h_1(x)$,

$\cdots, h_m(x)$ 是 $R(x)$ 中有限个非零元，且 P 是 $R(x)$ 的一个正锥，则有 $b, c \in R$, 使得 $b <_{R^2} c$, 且对于 R 的开区间 $]b, c[$ 中每个元 a, 下列事实成立：

(1) $h_1(a), \cdots, h_m(a)$ 都有意义，即在替换 $x = a$ 下，$h_1(x), \cdots, h_m(x)$ 的分母均不为零；

(2) $h_i(x)$ 关于 P 的符号与 $h_i(a)$ 关于 R^2 的符号相同，$i = 1, \cdots, m$.

证明 由于 $R(x)$ 是多项式环 $R[x]$ 的分式域，从而可设 $h_i(x) = \frac{f_i(x)}{f_0(x)}$, 其中 $f_i(x) \in R[x]$, 且 $f_i(x) \neq 0$, $i = 0, 1, \cdots, m$. 由定理 2.1.3 的推论知，这些多项式 $f_0(x), f_1(x), \cdots, f_m(x)$ 在 $R[x]$ 中都可分解成一次因式或二次不可约因式的乘积. 从而可令

$$f_i(x) = a_i(x-\alpha_1)^{e_{i1}} \cdots (x-\alpha_r)^{e_{ir}}[(x-b_1)^2 + c_1^2]^{d_{i1}} \cdots [(x-b_s)^2 + c_s^2]^{d_{is}},$$

其中 $a_i, \alpha_j, b_k, c_k \in R$, $c_k \neq 0$, $e_{ij}, d_{ik} \geqslant 0$, $i = 0, 1, \cdots, m$; $j = 1, \cdots, r$; $k = 1, \cdots, s$, 而且 $\alpha_1 <_{R^2} \alpha_2 <_{R^2} \cdots <_{R^2} \alpha_r$.

将元素 $\alpha_1, \cdots, \alpha_r$ 与 x 按序 $\leqslant_P$ 排列如下；

$$\alpha_1 <_{R^2} \cdots <_{R^2} \alpha_t <_P x <_P \alpha_{t+1} <_{R^2} \cdots <_{R^2} \alpha_r,$$

其中 $0 \leqslant t \leqslant r$.

当 $t = 0$ 时，令 $b = \alpha_1 - 1$, $c = \alpha_1$；当 $t = r$ 时，取 $b = \alpha_r$, $c = \alpha_r + 1$; 而当 $0 < t < r$ 时，取 $b = \alpha_t$, $c = \alpha_{t+1}$. 易知，对于每个 $a \in]b, c[$, $x - \alpha_i$ 关于 P 的符号相同于 $a - \alpha_i$ 关于 R^2 的符号，$(x-b_k)^2 + c_k^2$ 关于 P 的符号相同于 $(a-b_k)^2 + c_k^2$ 关于 R^2 的符号. 此时可知，引理中条件 (1) 和 (2) 都成立. 证毕.

引理 3.6.2 设 K 是域 F 上一个超越次数为 1 的函数域，ϕ 是 K 的一个代数 F- 位，则 ϕ 的值域 $\phi(K)$ 是 F 的一个有限扩张.

证明 任取 K 中一个在 F 上超越的元素 t, 则 K 是 $F(t)$ 的有限扩张.

不妨设 $\phi(t) \neq \infty$; 否则以 t^{-1} 代替 t. 此时可断言：$\phi(F(t)) = F(\phi(t))$. 事实上，对于任意 $\dfrac{f(t)}{g(t)} \in F(t)$, 其中 $f(t)$, $g(t)$ 是 $F[t]$ 中两个互素的多项式，使得 $\phi(\dfrac{f(t)}{g(t)}) \neq \infty$, $f(\phi(t)) = \phi(f(t)) = \phi(g(t))\phi(\dfrac{f(t)}{g(t)}) = g(\phi(t))\phi(\dfrac{f(t)}{g(t)})$. 假若 $g(\phi(t)) = 0$, 则 $f(\phi(t)) = 0$, 矛盾于 $f(t)$ 与 $g(t)$ 的互素性. 从而 $g(\phi(t)) \neq 0$, 进而有 $\phi(\dfrac{f(t)}{g(t)}) = \dfrac{f(\phi(t))}{g(\phi(t))} \in F(\phi(t))$. 因而 $\phi(F(t)) = F(\phi(t))$.

此外，由赋值论知识，$[\phi(K) : \phi(F(t))] \leqslant [K : F(t)]$. 从而 $\phi(K)$ 是 $\phi(F(t))$ 的有限扩张. 又由于 ϕ 是代数 F- 位，从而 $F(\phi(t))$ 是 F 的有限扩张. 因此，$\phi(K)$ 是 F 的有限扩张. 证毕.

定理 3.6.3(有理位的存在定理) 设 R 是一个实闭域，K 是 R 上一个实函数

域, 且 $z_1, \cdots, z_n$ 是 K 中任意有限个元素, 则存在一个有理 R- 位 ϕ: $K \longrightarrow R\cup\{\infty\}$, 使得 $\phi(z_i) \in R, i = 1, \cdots, n$.

证明 设 r 为 K 在 R 上的超越次数. 下面对 r 施用归纳法:

当 $r = 1$ 时, 令 $t = z_1^2 + \cdots + z_n^2$, 若 $z_1^2 + \cdots + z_n^2$ 在 R 上是超越元; 否则令 $t = z_1^2 + \cdots + z_n^2 + z^2$, 其中 z 是 R 上任意一个超越元. 显然, t 是 R 上超越元. 从而有 $K = R(t)(\alpha)$, 这里 α 是 $R(t)$ 上一个代数元. 设 α 在 $R(t)$ 上的极小多项式为: $f(x) = x^d + a_1(t)x^{d-1} + \cdots + a_d(t)$, 其中 $a_i(t) \in R(t), i = 1, \cdots, d$.

令 ρ_f 是如 §2.3 中由多项式 $f(x)$ 所确定的域 $R(t)$ 上二次型, 则经过一个非退化的线性替换后, ρ_f 可化成标准形: $\rho_f = b_1(t)y_1^2 + \cdots + b_d(t)y_d^2$, 其中 $b_1(t), \cdots, b_d(t) \in R(t)$.

由于 K 是一个实域, 从而 K 有一个正锥 Q_K. 令 $Q = Q_K \cap R(t)$, 则 $f(x)$ 在序域 $(R(t), Q)$ 的序代数扩张 (K, Q_K) 中有根 α. 由定理 2.3.3 知, $\mathrm{sgn}_Q(\rho_f) > 0$. 根据引理 3.6.1, 有 $a \in R$, 使得 $b_i(a)$ 有意义, 且 $b_i(t)$ 关于 Q 的符号相同于 $b_i(a)$ 关于 R^2 的符号, $i = 1, \cdots, d$. 按照定理 2.6.3, 设 Q_{a+} 是由 R 的分割 D_{a+} 所确定的 $R(t)$ 的正锥. 根据定理 2.6.3 可知, $b_i(t)$ 关于 Q_{a+} 的符号相同于 $b_i(a)$ 关于 R^2 的符号, $i = 1, \cdots, d$. 由此有 $\mathrm{sgn}_{Q_{a+}}(\rho_f) > 0$. 由定理 2.3.7 的推论知, Q_{a+} 可拓展为 K 的一个正锥 Q_1.

令 $A := \{\dfrac{f(t)}{g(t)} \mid f(t), g(t) \in R[t]$, 且 $g(a) \neq 0\}$. 易知 A 是域 $R(t)$ 的一个赋值环, 且 A 的赋值理想 $M = \{\dfrac{f(t)}{g(t)} \mid f(t), g(t) \in R[t], f(a) = 0$ 但 $g(a) \neq 0\}$. 据此, 作 $R(t)$ 到 $R \cup \{\infty\}$ 的映射 ψ, 使得对于任意两个互素的多项式 $f(t)$, $g(t) \in R[t]$, $\psi(\dfrac{f(t)}{g(t)}) = \dfrac{f(a)}{g(a)}$, 若 $\dfrac{f(t)}{g(t)} \in A$; 否则 $\psi(\dfrac{f(t)}{g(t)}) = \infty$. 易知, ψ 是 $R(t)$ 的一个 R- 位, 且 ψ 的赋值环为 A. 对于 $\dfrac{f(t)}{g(t)} \in M$, $g^2(t+a) - f(t+a)g(t+a)$ 的常项系数为 R 中正元素 $g^2(a)$. 从而 $g^2(t) - f(t)g(t) \in Q_{a+}$, 即 $1 - \dfrac{f(t)}{g(t)} \in Q_{a+}$. 由命题 3.1.3 知, A 关于正锥 Q_{a+} 是凸的. 此外, 由于 $A/M \cong R[t]/(t-a) \cong R$, 从而 ψ 的剩余域 A/M 是一个实闭域. 由引理 2.3.4 知, 由 ψ 所诱导的 A/M 到 R 的嵌入是保序的. 由定理 3.3.4 知, ψ 与 Q_{a+} 相容. 根据定理 3.3.5, ψ 可以拓展为 K 的一个 R- 值位 ϕ. 由于 $\phi(t) = \psi(t) = a \in R$, 从而 $t \in A_\phi$, 这里 A_ϕ 是 ϕ 的赋值环. 由 t 的规定有, $z_1^2 + \cdots + z_n^2 \in A_\phi$ 或 $z_1^2 + \cdots + z_n^2 + z^2 \in A_\phi$. 再由命题 3.1.2 的推论 1 知, $z_i \in A_\phi$ 即 $\phi(z_i) \in R, i = 1, \cdots, n$. 因此, 当 $r = 1$ 时, 定理成立.

假定对于超越次数为 $r-1$ 的实函数域, 定理成立. 现设 $K = R(\alpha_1, \cdots, \alpha_m)$ 在 R 上的超越次数为 r, 且 $t_1, \cdots, t_r$ 为 K 在 R 上一个超越基. 设 Q_K 是 K 的任意一个正锥, 且 R_1 是序域 (K, Q_K) 的实闭包. 令 $E = R(t_1, \cdots, t_{r-1})$, 且 R_0 是 E 在 R_1 中的代数闭包. 由命题 2.1.5 知, R_0 是一个实闭域. 注意到 $R_0 \subseteq R_0(\alpha_1, \cdots, \alpha_m) \subseteq R_1$.

从而 $R_0(\alpha_1,\cdots,\alpha_m)$ 是 R_0 上一个超越次数为 1 的实函数域. 由 $r=1$ 时的证明, 有一个从 $R_0(\alpha_1,\cdots,\alpha_m)$ 到 $R_0\cup\{\infty\}$ 的有理 R_0- 位 ψ_1, 使得 $\psi_1(z_i)\in R_0$, $i=1$, $\cdots,n$. 令 $\phi_1=\psi_1|_K$, 则 ϕ_1 显然是 K 的一个代数 E- 位. 注意到 K 是 E 上的超越次数为 1 的函数域. 由引理 3.6.2 知, $\phi_1(K)$ 是 E 的一个有限扩张, 从而是 R 上一个超越次数为 $r-1$ 的实函数域. 由归纳假定, 有一个从 $\phi_1(K)$ 到 $R\cup\{\infty\}$ 的有理 R- 位 ϕ_2, 使得 $\phi_2(\phi_1(z_i))\in R$, $i=1,\cdots,n$. 令 ϕ 是位 ϕ_1 和 ϕ_2 的合成, 即 $\phi=\phi_2\circ\phi_1$, 则 ϕ 是 K 的有理 R- 位, 使得 $\phi(z_i)\in R$, $i=1,\cdots,n$. 证毕.

为应用上需要, 上面的定理可以进一步改进, 使得有理位 ϕ 满足更多的所需要的条件.

定理 3.6.4 设 R 是一个实闭域, K 是 R 上一个实函数域, $z_1,\cdots,z_n$, $u_1,\cdots,u_m\in K$. 如果 K 有一个序 P, 使得 $0<_P u_j$, $j=1,\cdots,m$, 那么存在一个有理 R- 位 ϕ: $K\longrightarrow R\cup\{\infty\}$, 使得 $\phi(z_i)\in R$, $i=1,\cdots,n$, 且 $0<_{R^2}\phi(u_j)\in R$, $j=1,\cdots,m$.

证明 设 R_1 是序域 (K,P) 的实闭包. 由于 $u_j\in P\subseteq R_1^2$, 从而有 $v_j\in R_1$, 使得 $u_j=v_j^2$, $j=1,\cdots,m$. 令 $K_1=K(v_1,v_1^{-1},\cdots,v_m,v_m^{-1})$, 则 K_1 也是 R 上一个实函数域. 由定理 3.6.3 知, K_1 有一个有理 R- 位 ψ: $K_1\longrightarrow R\cup\{\infty\}$, 使得 $\psi(z_i)\in R$, $i=1,\cdots,n$, 且 $\psi(v_j)$, $\psi(v_j^{-1})\in R$, $j=1,\cdots,m$. 此时 $\psi(u_j)=\psi(v_j^2)=\psi(v_j)^2$, 且 $\psi(v_j)\psi(v_j^{-1})=\psi(1)=1$. 因而, $0<_{R^2}\psi(u_j)$, $j=1,\cdots,m$. 令 $\phi=\psi|_K$, 则 ϕ 满足定理中条件. 证毕.

当函数域的基域不是实闭域时, 上面定理可作如下相应的调整.

定理 3.6.5 设 K 是域 F 上一个实函数域, $z_1,\cdots,z_n,u_1,\cdots,u_m\in K$. 如果 P 是 K 的一个正锥, 使得 $0<_P u_j$, $j=1,\cdots,m$, 且 R 是序域 $(F,P\cap F)$ 的实闭包, 那么存在一个代数 F- 位 ϕ: $K\longrightarrow R\cup\{\infty\}$, 使得 $\phi(z_i)\in R$, $i=1,\cdots,n$, 且 $0<_{R^2}\phi(u_j)\in R$, $j=1,\cdots,m$.

证明 设 R_1 是序域 (K,P) 的实闭包, 且令 R_0 是 F 在 R_1 中的代数闭包. 由命题 2.1.5 知, R_0 实际上也是序域 $(F,P\cap F)$ 的实闭包. 由实闭包的惟一性, 存在 R_0 到 R 的一个保序的 F- 同构 π.

显然, $R_0(K)$ 是 R_0 上一个实函数域, 且它有一个正锥 $R_1^2\cap R_0(K)$, 使得 $u_j\in P\subseteq R_1^2\cap R_0(K)$, $j=1,\cdots,m$. 由定理 3.6.4 知, 存在一个有理 R_0- 位 ψ: $R_0(K)\longrightarrow R_0\cup\{\infty\}$, 使得 $\psi(z_i)\in R_0$, $i=1,\cdots,n$, 且 $0<_{R_0^2}\psi(u_j)\in R_0$, $j=1,\cdots,m$. 将 ψ 在 K 上的限制 $\psi|_K$ 与同构 π 合成, 则 $\phi:=\pi\circ\psi|_K$ 为所求. 证毕.

推论 设 K 是域 F 上实函数域, $\alpha_1,\cdots,\alpha_r$ 是 K 中非零元素, 则对于序空间 $\mathcal{X}_K$ 的每个非空开子集 W, 有 K 的一个非浅显实赋值 v, 使得如下条件成立: (1) 对于任意元素 $a\in\dot{F}$, $v(a)=0$; (2)$v(\alpha_i)=0$, $i=1,\cdots,r$; 且 (3)$W\cap\mathcal{X}_K^v\neq\phi$.

证明 对于 $\mathcal{X}_K$ 的任意非空的基本开子集 $H(a_1,\cdots,a_n)$, 有 F 的一个相应的实函数域 $L:=K(\sqrt{a_1},\cdots,\sqrt{a_n})$. 设 Q_1 是 L 的任意一个正锥, 且记 R 为序域 $(F,Q_1\cap F)$ 的实闭包. 由定理 3.6.5 知, 有一个代数 F- 位 ϕ: $L\longrightarrow R\cup\{\infty\}$, 使得 $\phi(\alpha_i)\in R$, 且 $\phi(\alpha_i)\neq 0$, $i=1,\cdots,r$. 令 w 是与位 ϕ 相对应的赋值. 由于 ϕ 是非浅显实位, 从而 w 是域 L 的一个非浅显实赋值. 由定理 3.1.4 知, 有某个 $Q\in\mathcal{X}_L$, 使得 w 与 Q 相容. 令 $v=w\,|_K$ 是 w 在 K 上的限制, 且 $P=Q\cap K$. 此时易知, v 满足上面的条件 (1) 和 (2), 且 $P\in H(a_1,\cdots,a_n)\cap\mathcal{X}_K^v$. 证毕.

作为有理位的存在定理的一个重要推论, 可以建立被称为 Lang 同态定理 的如下结果.

定理 3.6.6 设 L 是实闭域 R 的一个实扩张, 则对于 L 的任意一个在 R 上有限生成的子环 D, 总存在 D 到 R 的一个 R- 代数同态.

证明 设 K 是 D 在 L 中的分式域, 则 K 是 R 上实函数域. 由条件可设 $D=R[z_1,\cdots,z_n]$, 其中 $z_1,\cdots,z_n\in L$. 由定理 3.6.3 知, 存在一个有理 R- 位 ϕ: $K\longrightarrow R\cup\{\infty\}$, 使得 $\phi(z_i)\in R$, $i=1,\cdots,n$. 此时, $\phi\,|_D$ 显然是 D 到 R 的一个 R- 代数同态. 证毕.

同样, 定理 3.6.6 可作如下改进.

定理 3.6.7 设 L 是域 F 的一个实扩张, P 是 L 的一个正锥, 且 R 是序域 $(F,P\cap F)$ 的实闭包. 如果 D 是 L 的一个在 F 上有限生成的子环, 且 $0<_P u_j\in D$, $j=1,\cdots,m$, 则存在 D 到 R 的一个 F- 代数同态 ϕ, 使得 $0<_{R^2}\phi(u_j)$, $j=1,\cdots,m$.

证明 类似于定理 3.6.5 的证明.

由 Lang 同态定理, 容易建立如下重要引理.

引理 3.6.8 设 K 是实闭域 R 的一个扩张, P 是 K 的一个序, $f(x_1,\cdots,x_n)$ 是 R 上一个 n 元多项式, 且 $b_i,c_i\in R$, 其中 $b_i<_{R^2}c_i$, $i=1,\cdots,n$. 如果下面叙述成立: 对于任意 $y_1,\cdots,y_n\in R$, $f(y_1,\cdots,y_n)<_{R^2}0$, 只要 $b_i<_{R^2}y_i<_{R^2}c_i$, $i=1,\cdots,n$. 那么在序域 (K,P) 中, 如下相应的叙述也成立: 对于任意 $y_1,\cdots,y_n\in K$, $f(y_1,\cdots,y_n)<_P 0$, 只要 $b_i<_P y_i<_P c_i$, $i=1,\cdots,n$.

证明 如若不然, 则有某些 $y_1,\cdots,y_n\in K$, 使得 $b_i<_P y_i<_P c_i$, $i=1,\cdots,n$, 但 $f(y_1,\cdots,y_n)\geqslant_P 0$. 由定理 3.6.7 知, 有一个从 $R[y_1,\cdots,y_n]$ 到 R 的 R- 代数同态 ϕ, 使得 $b_i<_{R^2}\phi(y_i)<_{R^2}c_i$, $i=1,\cdots,n$, 但 $\phi(f(y_1,\cdots,y_n))\geqslant_{R^2}0$ 即 $f(\phi(y_1),\cdots,\phi(y_n))\geqslant_{R^2}0$, 矛盾于所设. 证毕.

作为有理位的存在定理的一个推广, M. Knebusch 建立了如下结果.

定理 3.6.9 设 K 是域 F 上函数域, $t_1,\cdots,t_r$ 是 K 在 F 上的一个超越基, $r\geqslant 1$, E 是包含 F 的一个实闭域, 且 R 是 F 在 E 中的代数闭包. 如果 F 的正锥 $E^2\cap F$ 可以拓展为 K 的一个正锥, 那么有 $b_i,c_i\in R$, 其中 $b_i<_{R^2}c_i$, $i=1,\cdots,$

r, 满足如下条件: 对于 E 中任意一组 r 个元素 $e_1, \cdots, e_r$, 只要 $b_i <_{E^2} e_i <_{E^2} c_i$, $i=1, \cdots, r$, 总有一个 F- 位 ϕ: $K \longrightarrow E \cup \{\infty\}$, 使得 $\phi(t_i) = e_i$, $i = 1, \cdots, r$.

证明 由所设知, F 的特征为零. 由本原元定理知, $K = F(t_1, \cdots, t_r)(\alpha)$, 其中 α 是域 $F(t_1, \cdots, t_r)$ 上的代数元. 设 α 在 $F(t_1, \cdots, t_r)$ 上的极小多项式为

$$f(x) := g(t_1, \cdots, t_r, x) = x^d + h_1 x^{d-1} + \cdots + h_d,$$

其中 $h_1, \cdots, h_d \in F(t_1, .., t_r)$.

如若 $h \in F[t_1, \cdots, t_r]$ 是有理函数 $h_1, \cdots, h_d$ 的一个公分母, 则易知 $h\alpha$ 在 $F(t_1, \cdots, t_r)$ 上的极小多项式的次数仍为 d, 且该极小多项式的全部系数都属于 $F[t_1, \cdots, t_r]$. 因而, 通过用 $h\alpha$ 代替 α 后, 可设 $h_1, \cdots, h_d \in F[t_1, \cdots, t_r]$.

记 $P = E^2 \cap F$, 且设 P 可拓展为 K 的一个正锥 Q. 令 R_1 是序域 (K, Q) 的实闭包, 则 $f(x)$ 在 R_1 中有根 α. 注意到, $f(x)$ 在 R_1 中不可能有重根. 从而易知, 有 $u, v \in R_1$, 使得 $f(u) <_{R_1^2} 0 <_{R_1^2} f(v)$.

设 R 是 F 在 E 中的代数闭包, 则由命题 2.1.5 知, R 是序域 (F, P) 的实闭包. 由定理 3.6.8 知, 存在一个 $D = F[t_1, \cdots, t_r, u, v]$ 到 R 的 F- 代数同态 ϕ, 使得 $\phi(f(u)) <_{R^2} 0 <_{R^2} \phi(f(v))$. 从而有 $g(a_1, \cdots, a_r, b) <_{R^2} 0 <_{R^2} g(a_1, \cdots, a_r, c)$, 其中 $b = \phi(u)$, $c = \phi(v)$, $a_i = \phi(t_i)$, $i = 1, \cdots, r$. 由命题 1.2.1 的推论 2 知, R 有一个正元素 δ, 使得下面的叙述成立: 对于任意$y_1, \cdots, y_r \in R$, 只要 $-\delta <_{R^2} y_i - a_i <_{R^2} \delta$, $i = 1, \cdots, r$, 总有$g(y_1, \cdots, y_r, b) <_{R^2} 0 <_{R^2} g(y_1, \cdots, y_r, c)$. 令 $b_i = a_i - \delta$, 而 $c_i = a_i + \delta$, $i = 1, \cdots, r$. 下面证明这些元素满足定理的要求.

设 $e_1, \cdots, e_r$ 是 E 中任意 r 个元素, 且 $b_i <_{E^2} e_i <_{E^2} c_i$, $i = 1, \cdots, r$. 任意取域 E 上 r 个代数无关的元素 $\eta_1, \cdots, \eta_r$, 且令 $L = E(\eta_1, \cdots, \eta_r)$. 按照定理 2.6.3, L 有一个正锥 Q, 使得 η_1 是在子域 E 上的正无限小元素, 而 η_i 是在子域 $E(\eta_1, \cdots, \eta_{i-1})$ 上的正无限小元素, $i = 2, \cdots, r$. 对于多项式环 $E[\eta_1, \cdots, \eta_r]$ 中全部项, 可规定一个字典序 $\preceq$, 使得 $\eta_1 \prec \eta_2 \prec \cdots \prec \eta_r$. 容易证明: 对于非零 $p \in E[\eta_1, \cdots, \eta_r]$, $0 <_Q p$ 当且仅当 p 关于字典序 $\preceq$ 的尾项系数为 E 中正元素. 对于 $\frac{p}{q} \in L$, 其中 p 和 q 是 $E[\eta_1, \cdots, \eta_r]$ 中非零多项式, 可按如下方式规定: 若 p 的尾项低于 q 的尾项, 则 $\psi(\frac{p}{q}) = \infty$; 若 p 的尾项高于 q 的尾项, 则 $\psi(\frac{p}{q}) = 0$; 若 p 和 q 有相同尾项, 则 $\psi(\frac{p}{q}) = \frac{a}{b}$, 其中 a 和 b 分别为 p 和 q 的尾项系数. 此外, 规定 $\psi(0) = 0$. 这样, 实际上规定了一个映射 ψ: $L \longrightarrow E \cup \{\infty\}$.

进一步可验证: ψ 是 L 的一个有理 E- 位. 设 $0 <_Q \frac{p}{q} <_Q \frac{p_1}{q_1}$, 且 $\psi(\frac{p_1}{q_1}) \neq \infty$. 必要时可通分, 从而可设 $q_1 = q \in Q$. 由于 $\psi(\frac{p_1}{q_1}) \neq \infty$, 从而 p_1 的尾项不低于 q 的尾项. 注意到 $0 <_Q p$, 且 $0 <_Q p_1 - p$. 因而, p 和 $p_1 - p$ 的尾项系数都为正. 从而 p 的尾项不低于 p_1 的尾项, 自然不低于 q 的尾项. 于是 $p_1 - p$ 的尾项不低于 q 的尾项. 由 ψ 的规定可知, $\psi(\frac{p}{q})$ 和 $\psi(\frac{p_1-p}{q})$ 关于正锥 E^2 都是 E 中非负元素. 从而

有 $0 \leqslant_{E^2} \psi(\frac{p}{q}) \leqslant_{E^2} \psi(\frac{p_1}{q})$. 因此, ψ 与 Q 相容.

令 R_1 是序域 (L, Q) 的实闭包. 由定理 3.3.6 知, ψ 可 (惟一地) 拓展为 R_1 的一个 E- 值位 Ψ.

由引理 3.6.8 知, 将域 R 扩大到 R_1, 上面的叙述仍然成立. 由正锥 Q 的规定知, $b_i <_Q e_i + \eta_i <_Q c_i$, $i = 1, \cdots, r$. 从而有 $g(e_1 + \eta_1, \cdots, e_r + \eta_r, b) <_{R^2} 0 <_{R^2} g(e_1 + \eta_1, \cdots, e_r + \eta_r, c)$.

由中间值定理知, 有 $\gamma \in R_1$, 使得 $g(e_1 + \eta_1, \cdots, e_r + \eta_r, \gamma) = 0$. 显然, $e_1 + \eta_1, \cdots, e_r + \eta_r$ 在 F 上是代数无关的. 从而, 存在 K 到 R_1 的这样一个 F- 嵌入 π, 使得 $\pi(t_i) = e_i + \eta_i$, $i = 1, \cdots, r$, 且 $\pi(\alpha) = \gamma$. 令 ϕ 是 π 与 Ψ 在 $\pi(K)$ 的限制 $\Psi|_{\pi(K)}$ 的合成, 则 ϕ 是 K 到 E 的一个 F- 位, 而且 $\phi(t_i) = \Psi(e_i + \eta_i) = e_i$, $i = 1, \cdots, r$. 证毕.

推论 设 K 是实闭域 R 上实函数域, $t_1, \cdots, t_r$ 是 K 在 R 上的一个超越基, $r \geqslant 1$, E 是包含 R 的一个实闭域, 则有 $b_i, c_i \in R$, 其中 $b_i <_{R^2} c_i$, $i = 1, \cdots, r$, 满足如下条件: 对于 E 中任意一组 r 个元素 $e_1, \cdots, e_r$, 只要 $b_i <_{E^2} e_i <_{E^2} c_i$, $i = 1, \cdots, r$, 总有一个 R- 位 ϕ: $K \longrightarrow E \cup \{\infty\}$, 使得 $\phi(t_i) = e_i$, $i = 1, \cdots, r$.

现在, 我们来讨论 Lang 的第三个重要结果 — 嵌入定理.

定理 3.6.10 设 K 是域 F 上一个超越次数为 r 的函数域, E 是 F 的一个实闭扩张, 且 E 在 F 上的超越次数 $\geqslant r$, 则存在一个从 K 到 E 的 F- 嵌入, 当且仅当 F 的正锥 $E^2 \cap F$ 可以拓展为 K 的一个正锥.

证明 必要性: 设 π 是 K 到 E 的一个 F- 嵌入. 令 $Q = \pi^{-1}(E^2)$, 则易知, Q 是 K 的一个正锥, 且有 $E^2 \cap F \subseteq Q$. 从而必要性成立.

充分性: 设 $t_1, \cdots, t_r$ 是 K 在 F 上的一个超越基, 且设 R 是 F 在 E 中的代数闭包. 根据定理 3.6.9, 有 $b_i, c_i \in R$, 其中 $b_i <_{R^2} c_i$, $i = 1, \cdots, r$, 满足如下条件: 对于 E 中任意一组 r 个元素 $e_1, \cdots, e_r$, 只要 $b_i <_{E^2} e_i <_{E^2} c_i$, $i = 1, \cdots, r$, 总有一个 F- 位 ϕ: $K \longrightarrow E \cup \{\infty\}$, 使得 $\phi(t_i) = e_i$, $i = 1, \cdots, r$.

由于 E 在 F 上的超越次数 $\geqslant r$, 从而 E 中有元素 $\beta_1, \cdots, \beta_r$, 且它们在 F 上代数无关. 令 $F_i = R(\beta_1, \cdots, \beta_i)$, $i = 0, 1, \cdots, r$. 由命题 1.4.4 知, 对于序域 $(F_i, E^2 \cap F_i)$ 的区间拓扑, $F_i \setminus F_{i-1}$ 是 F_i 的稠密子集, $i = 1, \cdots, r$. 从而有 $\alpha_i \in F_i \setminus F_{i-1}$, 使得 $b_i <_{E^2} \alpha_i <_{E^2} c_i$, $i = 1, \cdots, r$. 于是有一个 F- 位 ϕ: $K \longrightarrow E \cup \{\infty\}$, 使得 $\phi(t_i) = \alpha_i$, $i = 1, \cdots, r$. 记 ϕ_0 为位 ϕ 在 $F(t_1, \cdots, t_r)$ 上的限制. 由 $\alpha_1, \cdots, \alpha_r$ 的选取知, $\alpha_1, \cdots, \alpha_r$ 在 F 上是代数无关的. 从而可知, ϕ_0 实际是 $F(t_1, \cdots, t_r)$ 到 E 的一个嵌入, 即位 ϕ_0 是浅显的. 由于 K 是 $F(t_1, \cdots, t_r)$ 的代数扩张, 从而 ϕ 本身也是一个浅显位, 即 ϕ 是 K 到 E 的一个 F- 嵌入. 证毕.

推论 设 K 是实闭域 R 上一个超越次数为 r 的实函数域, E 是一个包含 R 的实闭域, 且 E 在 R 上的超越次数 $\geqslant r$, 则存在一个从 K 到 E 的 R- 嵌入.

第四章　Hilbert 第十七问题及其逆问题

在本章中，我们将在前面有关知识的基础上讨论著名的 Hilbert 第十七问题，并给出 E. Artin 对这一问题的的解答. 同时， Hilbert 第十七问题以一种更一般化的形式得到讨论，从而获得更普遍性的结论. 此外，我们研究了所谓的 Hilbert 第十七问题的逆问题，即研究使得 Hilbert 第十七问题得以成立的序域和亚序域.

§4.1　Hilbert 第十七问题与 Artin 的解答

1900 年，伟大数学家 D. Hilbert 在巴黎国际数学家会议上作了题为《数学问题》的著名讲话. 在这篇讲话中， Hilbert 提出了对以后的数学发展产生重大影响的著名的 23 个数学问题，其中第十七问题可叙述如下:

设 $f(x_1,\cdots,x_n)\in\mathbb{R}[x_1,\cdots,x_n]$ 是一个实系数 n 元多项式，使得对于任意 $a_1,\cdots,a_n\in\mathbb{R}$, 均有 $f(a_1,\cdots,a_n)\geqslant 0$. 问：多项式 $f(x_1,\cdots,x_n)$ 是否一定可表为 $\mathbb{R}(x_1,\cdots,x_n)$ 中若干个有理函数的平方和？

当 $n=1$ 时，根据定理 2.1.3 的推论可知，满足如上条件的单元多项式 $f(x)$ 可表示为两个实系数单元多项式的平方和. 当 $n=2$ 时， Hilbert 本人也对上述问题给出了肯定的证明.

Hilbert 第十七问题 的第一个正面的解答，是由 E. Artin 在 1926 年获得的. Artin 的解答是建立在他与 O. Schreier 共同建立的实域理论的基础上，这些理论及其思维方法渗透在前面的有关章节中.

实际上， Artin 的正面解答是一个比 Hilbert 第十七问题的原形式更为精致的结果. 在这里，为简明起见，我们不照搬 Artin 的原始证明方法，而应用前面的 Lang 同态定理.

定理 4.1.1(Artin)　设域 F 仅有惟一的正锥 P, 且 P 是一个阿基米德正锥. 若 $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$, 使得对于任意 $a_1,\cdots,a_n\in F$, $f(a_1,\cdots,a_n)\geqslant_P 0$, 则 $f(x_1,\cdots,x_n)$ 可表为 $F(x_1,\cdots,x_n)$ 中若干个有理函数的平方和.

证明　设 R 是序域 (F,P) 的实闭包，则由定理 1.4.2 知， R 的惟一序 $\leqslant_{R^2}$ 是一个阿基米德序.

假若 $f(x_1,\cdots,x_n)$ 不能表示为 $F(x_1,\cdots,x_n)$ 中若干个有理函数的平方和，则 $f(x_1,\cdots,x_n)\notin S_{F(x_1,\cdots,x_n)}$, 这里 $S_{F(x_1,\cdots,x_n)}$ 是有理函数域 $F(x_1,\cdots,x_n)$ 的弱亚正锥. 由定理 1.1.2 知，存在 $F(x_1,\cdots,x_n)$ 的一个正锥 Q, 使得 $f(x_1,\cdots,x_n)\notin Q$, 即 $f(x_1,\cdots,x_n)<_Q 0$.

由 Lang 同态定理 (定理 3.6.7) 知，有 $F[x_1,\cdots,x_n]$ 到 R 的一个 F- 代数同态 ϕ, 使得 $\phi(f(x_1,\cdots,x_n))<_{R^2} 0$, 即 $f(\alpha_1,\cdots,\alpha_n)<_{R^2} 0$, 其中 $\alpha_i=\phi(x_i)$, $i=$

$1, \cdots, n$. 由多项式函数的连续性知, R 有一个正元素 δ, 使得对于任意 $y_i \in R$, 只要 $-\delta <_{R^2} y_i - \alpha_i <_{R^2} \delta$, $i = 1, \cdots, n$, 恒有 $f(y_1, \cdots, y_n) <_{R^2} 0$.

由于序 $\leqslant_{R^2}$ 是阿基米德序, 从而由命题 1.4.3 知, 对于 R 上的区间拓扑, F 在 R 中稠密. 于是有 $a_1, \cdots, a_n \in F$, 使得 $-\delta <_{R^2} a_i - \alpha_i <_{R^2} \delta$. 此时有, $f(a_1, \cdots, a_n) <_{R^2} 0$, 即 $f(a_1, \cdots, a_n) <_P 0$, 矛盾于所设. 证毕.

当 $F = \mathbb{R}$ 时, 显然实数域 $\mathbb{R}$ 满足上面定理中的条件. 因此, 上面的 Artin 定理以更为一般的形式肯定地回答了 Hilbert 第十七问题.

注意到有理数域 $\mathbb{Q}$ 仅有惟一序, 且该序显然是阿基米德的. 从而由定理 4.1.1 立即可建立下面的推论:

推论　设 $f(x_1, \cdots, x_n)$ 是 $\mathbb{Q}[x_1, \cdots, x_n]$ 中一个多项式, 使得对于任意 $a_1, \cdots, a_n \in \mathbb{Q}$, $f(a_1, \cdots, a_n) \geqslant 0$, 则 $f(x_1, \cdots, x_n)$ 可表为 $\mathbb{Q}(x_1, \cdots, x_n)$ 中若干个有理函数的平方和.

由于 Lang 同态定理适用于任意实域上的实函数域, 并不要求这个实域的序满足其他附加条件 (比如, 是否为阿基米德序), 因而, Hilbert 第十七问题及其解答可在一种更一般的形式下进行讨论. 对此, 我们需要如下定义.

定义 4.1.1　设 (F, T) 是一个亚序域, $f(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$. 若对于任意 $a_1, \cdots, a_n \in F$, 都有 $f(a_1, \cdots, a_n) \in T$, 则称多项式 $f(x_1, \cdots, x_n)$ 在 (F, T) 上是半正定的. 若 f 和 $-f$ 在 (F, T) 上都不是半正定的, 则称 f 在 (F, T) 上是不定的. 特别地, 可定义序域 (F, P) 上的半正定和不定多项式.

定义 4.1.2　设 (F, T) 是一个亚序域, $f(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$. 若对于 (F, T) 的每个实闭包 R, $f(x_1, \cdots, x_n)$ 在序域 (R, R^2) 上半正定, 则称 $f(x_1, \cdots, x_n)$ 在 (F, T) 上强半正定. 特别地, 可定义序域 (F, P) 上的强半正定多项式.

显然, 强半正定多项式必是半正定的, 但反之未必. 此外易知, 多项式 f 在亚序域 (F, T) 上半正定 (强半正定), 当且仅当对于每个 $P \in \mathcal{X}_F(T)$, f 在序域 (F, P) 上半正定 (强半正定).

由定理 4.1.1 及其证明, 可以建立下面稍为一般的结果.

定理 4.1.2　设 (F, T) 是一个亚序域, 且 F 在 (F, T) 的每个实闭包中稠密, 则 (F, T) 上每个半正定 n 元多项式 f 可表为如下形式:

$$f = \sum_{i=1}^{m} t_i h_i^2,$$

其中 $t_i \in T$, $h_i \in F(x_1, \cdots, x_n)$, $i = 1, \cdots, m$.

证明　如若不然, 则有某个在 (F, T) 上半正定的多项式 $f(x_1, \cdots, x_n)$, 使得 f 不能表为如定理所示的形式. 作域 $F(x_1, \cdots, x_n)$ 的如下子集:

$$\widehat{T}=\left\{\sum_{i=1}^{m}t_ih_i^2 \mid m\text{为自然数}, t_i\in T,\ h_i\in F(x_1,\cdots,x_n),\ i=1,\cdots,m\right\}.$$

易知, $\widehat{T}$ 是域 $F(x_1,\cdots,x_n)$ 的一个亚正锥, 且 $f\notin\widehat{T}$. 由定理 1.1.2 知, $F(x_1,\cdots,x_n)$ 有一个正锥 Q, 使得 $0<_Q f$. 令 R 是序域 $(F,Q\cap F)$ 的实闭包. 显然 $T\subseteq Q\cap F$, 即 R 是 (F,T) 的一个实闭包. 由 Lang 同态定理 (定理 3.6.7) 可知, 有 $\alpha_1,\cdots,\alpha_n\in R$, 使得 $f(\alpha_1,\cdots,\alpha_n)<_{R^2}0$. 根据多项式函数的连续性以及 F 在 R 中的稠密性可知, 有 $a_1,\cdots,a_n\in F$, 使得 $f(a_1,\cdots,a_n)<_{R^2}0$, 即 $f(a_1,\cdots,a_n)\notin R^2$. 注意到, $T\subseteq R^2$. 从而 $f(a_1,\cdots,a_n)\notin T$, 矛盾于 f 的半正定性. 证毕.

推论 1 设 F 是一个实域, 且 F 在它的每个实闭包中稠密, $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$. 若对于每个 $P\in\mathcal{X}_F$, $f(x_1,\cdots,x_n)$ 在 (F,P) 上半正定, 则多项式 $f(x_1,\cdots,x_n)$ 可表为 $F(x_1,\cdots,x_n)$ 中若干个有理函数的平方和.

证明 将定理 4.1.2 应用于情况 $T=S_F$.

推论 2 设 (F,P) 是一个阿基米德序域, 则对于 (F,P) 上的每个半正定 n 元多项式 f,

$$f=\sum_{i=1}^{m}p_ih_i^2,$$

其中 $p_i\in P$, $h_i\in F(x_1,\cdots,x_n)$, $i=1,\cdots,m$.

在上面结论中, 所设的条件都含有或蕴含 "在实闭包中稠密" 这一条款. 下面的例子表明: 对于半正定多项式的平方和表示, "在实闭包中稠密" 这一条款并不是多余的.

例 设 $F=\mathbb{R}(t)$, 其中 t 是实数域 $\mathbb{R}$ 上一个超越元. 由定理 2.6.3, F 有一个正锥 P, 使得 t 在 $\mathbb{R}$ 上是正的无限小元素. 令 $f(x)=(x^2-t)^2-t^3$, 则可断言: $f(x)$ 在 (F,P) 上是半正定的. 事实上, 如若不然, 则有 $\dfrac{u(t)}{v(t)}\in F$, 其中 $u(t),v(t)\in\mathbb{R}[t]$, 且 $v(t)\neq 0$, 使得 $f(\dfrac{u(t)}{v(t)})<_P 0$. 由于 $f(0)=t^2-t^3>_P 0$, 从而 $u(t)\neq 0$. 于是可进一步假定: $u(t)$ 与 $v(t)$ 互素. 注意到 $[u^2(t)-tv^2(t)]^2<_P t^3v^4(t)$. 从而 $u^2(t)-tv^2(t)$ 的常项必为零, 即有 $u(0)=0$. 令 $u(t)=tu_1(t)$, 其中 $u_1(t)\in\mathbb{R}[t]$. 由此又有, $[tu_1^2(t)-v^2(t)]^2<_P tv^4(t)$. 从而又知, $tu_1^2(t)-v^2(t)$ 的常项为零. 从而有 $v(0)=0$, 矛盾于 $u(t)$ 与 $v(t)$ 的互素性. 因此, $f(x)$ 在 (F,P) 上是半正定的.

然而, $f(\sqrt{t})=-t^3<_P 0$, 这里 $\sqrt{t}$ 是多项式 x^2-t 在 (F,P) 的实闭包 R 中一个正根. 这表明: $f(x)$ 在 (F,P) 上不是强半正定的. 由下面的定理可知, $f(x)$ 不能表示为定理 4.1.2 中所示的平方和. 究其原因, 自然是因为 F 在 R 中不稠密. 事实上, 易知 R 中开区间 $]\sqrt{t},2\sqrt{t}[$ 不含有 F 中元素.

作为一个不含有措辞 "稠密性" 的一般性结论, 可建立下面的定理.

定理 4.1.3 设 (F,T) 是一个亚序域, $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$, 则多项式 $f(x_1,\cdots,x_n)$ 在 (F,T) 上是强半正定的, 当且仅当 f 可表为

$$f=\sum_{i=1}^{m}t_ih_i^2,$$

其中 $t_i\in T$, $h_i\in F(x_1,\cdots,x_n)$, $i=1,\cdots,m$.

证明 充分性: 设多项式 $f(x_1,\cdots,x_n)$ 可表为如上所示的平方和. 假若 f 在 (F,T) 上不是强半正定的, 则有 (F,T) 的某个实闭包 R 以及 $a_1,\cdots,a_n\in R$, 使得 $f(a_1,\cdots,a_n)<_{R^2}0$. 由多项式函数的连续性知, R 中有正元素 δ, 使得对于任意 $y_1,\cdots,y_n\in R$, $f(y_1,\cdots,y_n)<_{R^2}0$, 只要 $-\delta<_{R^2}y_i-a_i<_{R^2}\delta$, $i=1,\cdots,n$.

由于 R 中区间 $]a_i-\delta,a_i+\delta[_{R^2}$ 含有无限多个元素, 从而有 $b_1,\cdots,b_n\in]a_i-\delta,a_i+\delta[_{R^2}$, 使得对于代换 $x_i=b_i$, $i=1,\cdots,n$, $h_1,\cdots,h_m$ 的分母均不为零. 从而有 $f(b_1,\cdots,b_n)=\sum\limits_{i=1}^{m}t_ih_i^2(b_1,\cdots,b_n)$. 该等式左端对于序 $\leqslant_{R^2}$ 为负, 而右端为非负, 矛盾. 因此, f 在 (F,T) 上是强半正定的.

必要性: 设 f 在 (F,T) 上是强半正定的, 且令 $\widehat{T}=\{\sum\limits_{i=1}^{m}t_ih_i^2\mid m$ 为自然数, $t_i\in T$, 且 $h_i\in F(x_1,\cdots,x_n)$, $i=1,\cdots,m\}$.

假若 f 不能表为如上所示的平方和, 则 $f\notin\widehat{T}$. 此时知, $\widehat{T}$ 是域 $F(x_1,\cdots,x_n)$ 的一个亚正锥. 由定理 1.1.2 知, $F(x_1,\cdots,x_n)$ 有一个正锥 Q, 使得 $f<_Q0$. 由定理 4.1.2 的证明知, (F,T) 有一个实闭包 R 以及 $\alpha_1,\cdots,\alpha_n\in R$, 使得 $f(\alpha_1,\cdots,\alpha_n)<_{R^2}0$; 这矛盾于多项式 $f(x_1,\cdots,x_n)$ 在 (F,T) 上的强半正定性. 从而必要性获证. 证毕.

推论 1 设 (F,P) 是一个序域, 且 $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$, 则多项式 $f(x_1,\cdots,x_n)$ 在 (F,P) 的实闭包上是半正定的, 当且仅当 f 可表为

$$f=\sum_{i=1}^{m}p_ih_i^2,$$

其中 $p_i\in P$, $h_i\in F(x_1,\cdots,x_n)$, $i=1,\cdots,m$.

推论 2 设 R 是一个实闭域, $f(x_1,\cdots,x_n)\in R[x_1,\cdots,x_n]$, 则 $f(x_1,\cdots,x_n)$ 在 (R,R^2) 上是半正定的, 当且仅当 f 可表为

$$f=\sum_{i=1}^{m}h_i^2,$$

其中 $h_i\in R(x_1,\cdots,x_n)$, $i=1,\cdots,m$.

作为 Hilbert 第十七问题在实函数域上的一个推广, S. Lang 建立了下面结

果.

定理 4.1.4 设 K 是域 F 上一个实函数域，T 是 F 的一个亚正锥，则对于 $\alpha \in K$, 下列叙述等价：

(1) α 可表为 $\alpha = \sum_{i=1}^{m} t_i\beta_i^2$, 其中 m 为自然数，$t_i \in T, \beta_i \in K, i = 1, \cdots, m$;

(2) 对于 K 的每个代数的实 F- 位 ϕ 以及 $\phi(K)$ 的每个包含 T 的正锥 Q, $\phi(\alpha) = \infty$ 或 $\phi(\alpha) \geqslant_Q 0$.

证明 (1) $\Longrightarrow$ (2): 设 ϕ 是 K 的任意一个代数的实 F- 位，Q 是 $\phi(K)$ 的一个正锥，使得 $T \subseteq Q$. 若 $\phi(\alpha) \neq \infty$, 则 $\alpha \in A_\phi$, 这里 A_ϕ 是位 ϕ 的赋值环. 由定理 3.3.3 知，K 有一个正锥 P, 使得 ϕ 与 $\leqslant_P$ 和 $\leqslant_Q$ 相容. 注意到，对于每个非零 $t \in T, \phi(t) = t \in Q$. 由 ϕ 与 $\leqslant_P$ 和 $\leqslant_Q$ 的相容性知，对于每个非零 $t \in T, t \in P$. 从而 $T \subseteq P$. 由叙述 (1) 知，$\alpha \in P$. 由于 $\phi(\alpha) \neq \infty$, 从而由 ϕ 与 $\leqslant_P$ 和 $\leqslant_Q$ 的相容性知，$\phi(\alpha) \in Q$, 即 $0 \leqslant_Q \phi(\alpha)$.

(2) $\Longrightarrow$ (1): 令 $\widehat{T} = \{\sum_{i=1}^{m} t_i\beta_i^2 \mid m$ 为自然数，$t_i \in T, \beta_i \in K, i = 1, \cdots, m\}$. 假若叙述 (1) 不成立，则 $\alpha \notin \widehat{T}$. 此时易知，$\widehat{T}$ 是 K 的一个亚正锥，使得 $T \subseteq \widehat{T}$. 由定理 1.1.2 知，K 有一个正锥 P, 使得 $\widehat{T} \subseteq P$, 但 $\alpha \notin P$, 即 $\alpha <_P 0$. 令 R 是序域 $(F, P\cap F)$ 的实闭包. 由定理 3.6.5 知，存在 K 的一个代数 F- 位 ϕ, 使得 $\phi(\alpha) \in R$, 且 $\phi(\alpha) <_{R^2} 0$. 此时，$R^2 \cap \phi(K)$ 是 $\phi(K)$ 的一个正锥，且 $T \subseteq R^2 \cap F \subseteq R^2 \cap \phi(K)$; 这矛盾于叙述 (2). 因而，叙述 (1) 成立. 证毕.

§4.2 具有 Hilbert 性质的序域和 McKenna 定理

从定理 4.1.1 及其推论可见，对于不少有惟一序 P 的域 F, (F, P) 上的半正定多项式可以是有理函数的平方和. 尽管上节的例子表明，对于一个序域 (F, P), 如果 F 在它的实闭包内不是稠密的，那么 (F, P) 上的半正定多项式不一定可表成有理函数的平方和. 不过，该例子中的域 F 除 P 外还有无限多个序. 因而，历史上曾经有人产生这样一个误解：(F, P) 上的半正定多项式总是有理函数的平方和，只要 P 是 F 的惟一序. 但不久之后，D. W. Dubois 用下面的例子否决了这一误解.

例 设 $E = \mathbb{Q}(t)$, 其中 t 是有理数域 $\mathbb{Q}$ 上的一个超越元. 由定理 2.6.4 知，E 有一个正锥 P, 使得 t 成为在 $\mathbb{Q}$ 上的正无限小元素，即对于所有的正有理数 q, 都有 $0 <_P t <_P q$. 令 R 是 (E, P) 的实闭包，且设 F 是 E 在 R 中的平方闭包 (即 E 通过开平方运算而得出的在 R 中最大扩域). 此时，F 显然只有惟一的序 F^2.

考虑 $F[x]$ 中多项式 $f(x) = (x^3 - t)^2 - t^3$. 多项式 $f(x)$ 不是一个强半正定多项式，因为 $f(\sqrt[3]{t}) = -t^3 <_{R^2} 0$, 这里 $\sqrt[3]{t}$ 是多项式 $x^3 - t$ 在 R 中的正根. 因此，由

定理 4.1.3 知，在 $F(x)$ 中 $f(x)$ 不能表为平方和.

另一方面，能够证明：上面的多项式 $f(x)$ 是 (F, F^2) 上的一个半正定多项式. 今假设多项式 $f(x)$ 在 F 上不是半正定的，于是对于某个 $\alpha \in F$, $f(\alpha) <_{F^2} 0$. 从而有 $t - \sqrt{t^3} <_{F^2} \alpha^3 <_{F^2} t + \sqrt{t^3}$. 对于非零 $\frac{g}{h} \in E$, 其中 $g, h \in \mathbb{Q}[t]$, 规定 $v(\frac{g}{h}) = g$ 的尾项的次数 $-h$ 的尾项的次数. 此外规定，$v(0) = \infty$. 易知，v 是 E 的一个值群为 $\mathbb{Z}$ 的赋值，使得 $v(t) = 1$. 进一步可知，v 与序 P 相容. 由定理 3.2.4 知，v 可拓展为 F 的一个实赋值 w, 使得 w 与正锥 F^2 相容. 由 w 与正锥 F^2 的相容性有，$w(t - \sqrt{t^3}) \geqslant w(\alpha^3) \geqslant w(t + \sqrt{t^3})$, 即 $1 \geqslant 3w(\alpha) \geqslant 1$. 从而，$3w(\alpha) = 1$. 由于 F 是由 E 经开平方运算而得到的 R 中的子扩张，故存在有限个 F 的子域 $E_1, \cdots, E_r$, 使得 $E_r \supset E_{r-1} \supset \cdots \supset E_1 \supset E_0 = E$, 且 $\alpha \in E_r$, 其中 E_i 是 E_{i-1} 的二次扩张，$i = 1, \cdots, r$. 显然 $w(\alpha) \notin \mathbb{Z} = w(\dot{E})$, 但 $w(\alpha) \in w(\dot{E}_r)$. 从而可选取尽可能小的自然数 s, $1 \leqslant s \leqslant r$, 使得 $w(\alpha) \in w(\dot{E}_s)$, 但 $w(\alpha) \notin w(\dot{E}_{s-1})$. 由赋值论知识，$w(\dot{E}_{s-1})$ 是 $w(\dot{E}_s)$ 的一个子群，且指标 $[w(\dot{E}_s) : w(\dot{E}_{s-1})] \leqslant 2$. 从而有，$2w(\alpha) \in w(\dot{E}_{s-1})$. 于是，$w(\alpha) = 1 - 2w(\alpha) \in w(\dot{E}_{s-1})$, 矛盾. 因而，多项式 $f(x)$ 是 (F, F^2) 上的一个半正定多项式.

上面例子自然引起了这样的思考：对于一个序域 (F, P), 要使得其上的半正定多项式 (含有任意多个未定元) 能表成 F 上有理函数的平方和，应对该序域赋予什么条件？换言之，一个序域应具有何种性质，才能保证相应的第十七问题有肯定的解答？这一问题在当前文献中被称为 Hilbert 第十七问题的逆问题.

在上节中，定理 4.1.3 及其推论只给出了一些充分条件. 在第十七问题获得解答后的一段时期内，人们并不知道哪些条件是既充分又必要的. K. McKenna 于 20 世纪 70 年代中期考虑了上述逆问题，并就序域的情形获得解答. 在本节中，我们将介绍 McKenna 所讨论的序域情形. 在以后的两节中，将对问题作一般性的讨论. 为叙述上的方便，McKenna 引进了下面的概念.

定义 4.2.1 设 (F, P) 是一个序域. 若对于每个正整数 n, (F, P) 上每个 n 元半正定的多项式 $f(x_1, \cdots, x_n)$ 都可以表成 $F(x_1, \cdots, x_n)$ 中有理函数的平方和，则称 (F, P) 具有 Hilbert 性质 .

若对于每个正整数 n, (F, P) 上每个 n 元半正定的多项式 $f(x_1, \cdots, x_n)$ 都可以表成如下形式：

$$f = \sum_{i=1}^{m} p_i h_i^2,$$

其中 m 为自然数，$p_i \in P$, $h_i \in F(x_1, \cdots, x_n)$, $i = 1, \cdots, m$, 则称 (F, P) 具有弱 Hilbert 性质 .

为使研究更一般化，上面的定义可推广到亚序域的范畴中.

定义 4.2.2 设 (F,T) 是一个亚序域. 若对于每个正整数 n, (F,T) 上每个 n 元半正定的多项式 $f(x_1,\cdots,x_n)$ 都可以表成 $F(x_1,\cdots,x_n)$ 中有理函数的平方和, 则称 (F,T) 具有 Hilbert 性质 .

若对于每个正整数 n, (F,T) 上每个 n 元半正定的多项式 $f(x_1,\cdots,x_n)$ 都可以表成如下形式:

$$f=\sum_{i=1}^{m}t_ih_i^2,$$

其中 m 为自然数, $t_i\in T$, $h_i\in F(x_1,\cdots,x_n)$, $i=1,\cdots,m$, 则称 (F,T) 具有弱 Hilbert 性质 .

首先, 我们可建立如下一个很简单的刻画.

命题 4.2.1 (1) 亚序域 (F,T) 具有弱 Hilbert 性质, 当且仅当对于每个正整数 n, (F,T) 上的 n 元半正定多项式同时是强半正定的.

(2) 亚序域 (F,T) 具有 Hilbert 性质, 当且仅当亚序域 (F,T) 具有弱 Hilbert 性质, 且 T 是域 F 的弱亚正锥, 即 $T=S_F$.

证明 (1) 设亚序域 (F,T) 具有弱 Hilbert 性质. 如果 f 是 (F,T) 上一个 n 元半正定多项式, 则 f 可表成如定义 4.2.2 所示的形式. 由定理 4.1.3 知, f 在 (F,T) 上是强半正定的.

反过来, 若 (F,T) 上的 n 元半正定多项式 f 同时是强半正定的, 则由定理 4.1.3 知, f 可表成如定义 4.2.2 所示的形式. 由定义 4.2.2 知, 亚序域 (F,T) 具有弱 Hilbert 性质.

(2) 如果 (F,T) 具有 Hilbert 性质, 则 (F,T) 显然具有弱 Hilbert 性质. 此外, T 中任何元作为 (F,T) 上的半正定多项式得以表为平方和. 因此有 $T=S_F$.

反过来, 设亚序域 (F,T) 具有弱 Hilbert 性质, 且 $T=S_F$. 如果 f 是 (F,T) 上一个 n 元半正定多项式, 则 f 可表成如定义 4.2.2 所示的形式. 由于 $T=S_F$, 从而 f 实际上可以表成 $F(x_1,\cdots,x_n)$ 中有理函数的平方和. 这表明: (F,T) 具有 Hilbert 性质. 证毕.

推论 序域 (F,P) 具有 Hilbert 性质, 当且仅当对于每个正整数 n, (F,P) 上的 n 元半正定多项式同时是强半正定的, 并且 P 是 F 的惟一序.

McKenna 的工作是对具有 Hilbert 性质或弱 Hilbert 性质的序域作出刻画. 为论证的需要, 首先引进一些有关的概念.

定义 4.2.3 设 R 是序域 (F,P) 的实闭包, $\alpha\in R$. 若对于某个正元素 $c\in P$, R 中开区间 $]\alpha-c,\alpha+c[_{R^2}$ 不包含 F 的元素, 则称 α 是关于 F 的孤立元 . 此时, 又称 $]\alpha-c,\alpha+c[_{R^2}$ 与 F 是分离的. 非孤立元又称为关于 F 的极限元 .

显然，F 对于由 R^2 所诱导的区间拓扑不是 R 的稠密子集，当且仅当 R 中有关于 F 的孤立元. 孤立元在 F 上的极小多项式的次数必定大于 1.

为获得有关极限元的有关事实，我们需要建立下面的引理.

引理 4.2.2 设 R 是序域 (F,P) 的实闭包，则 R 中所有关于 F 的极限元组成一个包含 F 的子域.

证明 用 $\widetilde{F}$ 表示由 R 中全体关于 F 的极限元所组成的子集. 显然，$F\subseteq\widetilde{F}$. 设 $\alpha,\beta\in R$ 是任意两个关于 F 的极限元. 对于每个正元素 $c\in P$, 由所设知，总有 $a,b\in F$, 使得 $\alpha-\dfrac{c}{2}<_{R^2}a<_{R^2}\alpha+\dfrac{c}{2}$, 且 $\beta-\dfrac{c}{2}<_{R^2}b<_{R^2}\beta+\dfrac{c}{2}$. 从而有 $\alpha-\beta-c<_{R^2}a-b<_{R^2}\alpha-\beta+c$, 即开区间 $]\alpha-\beta-c,\alpha-\beta+c[_{R^2}$ 包含 F 的元素 $a-b$. 从而 $\alpha-\beta\in\widetilde{F}$. 进一步设 $\beta\neq 0$. 由引理 1.2.2 知，有 $M\in S_F\subseteq P$, 使得 $-M<\beta^{-1}<M$. 对于每个正元素 $c\in P$, 令 $c_1=\min\{\dfrac{1}{2M},\dfrac{c}{2M^2}\}$. 由所设知，总有 $b\in F$, 使得 $\beta-c_1<_{R^2}b<_{R^2}\beta+c_1$. 此时，$|b|\geqslant_{R^2}|\beta|-|\beta-b|>M^{-1}-\frac{1}{2M}=\frac{1}{2M}$. 显然 $b\neq 0$. 由此有，$|\beta^{-1}-b^{-1}|=|\beta-b||b\beta|^{-1}<c$. 这表明：$\beta^{-1}\in\widetilde{F}$. 再由引理 1.2.2 可知，有 $M_1\in S_F\subseteq P$, 使得 $-M_1<\beta<M_1$, 且 $-M_1<\alpha<M_1$. 对于每个正元素 $c\in P$, 令 $c_2=\min\{\dfrac{c}{3M_1},\dfrac{c}{3},1\}$. 由所设知，总有 $a,b\in F$, 使得 $\alpha-c_2<_{R^2}a<_{R^2}\alpha+c_2$, 且 $\beta-c_2<_{R^2}b<_{R^2}\beta+c_2$. 由此可得 $-c+\alpha\beta<_{R^2}ab<_{R^2}\alpha\beta+c$. 从而 $\alpha\beta\in\widetilde{F}$. 因此，$\widetilde{F}$ 是 R 的一个子域. 证毕.

以下始终用 $\widetilde{F}$ 表示由 R 中全体关于 F 的极限元所组成的子域. 显然 F 在 $\widetilde{F}$ 内是稠密的. 容易证明，R 中关于 $\widetilde{F}$ 的极限元必是关于 F 的极限元，从而属于 $\widetilde{F}$.

现设 (F,P) 是一个序域，R 是 F 的一个实闭扩张，使得 $P\subseteq R^2$, 且令 $\Omega=R(\sqrt{-1})$. 按定理 2.1.3, $\Omega=R(\sqrt{-1})$ 是一个代数闭域. 从而对于 Ω 中每个元素 z, 可惟一地写为：$z=a+b\sqrt{-1}$, 其中 a,b 都属于 R. 此时，我们可规定 z 关于正锥 R^2 的绝对值 $|z|_{R^2}$ 如下：

$$|z|_{R^2}=\sqrt{a^2+b^2}\in R,$$

这里 $\sqrt{a^2+b^2}$ 表示多项式 $x^2-(a^2+b^2)$ 在 R 中惟一的非负根.

容易验证，如上规定的 $|\cdot|_{R^2}$ 具有和通常复数的绝对值相类似的性质. 为简便起见，在不引起误解的情况下，记号 $|\cdot|_{R^2}$ 常简写为 $|\cdot|$.

引理 4.2.3 所设同上，又设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n\in F[x]$, 其中 $a_i\in F$, $i=0,1,\cdots,n$, 且 $a_0\neq 0$. 如果 $z_1,\cdots,z_r$ 为 $f(x)$ 在 Ω 中重数分别为 $m_1,\cdots,m_r$ 的全部相异的根，且 c 是 P 中一个正元素，使得 $c<_{R^2}\min\{\frac{1}{2}|z_i-z_j|\mid 1\leqslant i<j\leqslant r\}$, 则必有某个正元素 $\delta\in P$, 使得对于 $F[x]$ 中任意多项式 $g(x)=b_0x^n+b_1x^{n-1}+\cdots+b_n$, $g(x)$ 在 Ω 中恰有 m_j 个根 y, 满足 $|z_j-y|<_{R^2}c$, $j=1,\cdots,r$, 只要 $|b_i-a_i|<_{R^2}\delta$, $i=0,1,\cdots,n$.

证明 记 R_0 为 F 在 R 中的代数闭包. 由命题 2.1.5 知, R_0 实际上是 (F,P) 的实闭包. 显然, $1+|z_1|+\cdots+|z_1|^n \in R_0$. 根据引理 1.2.2, 有 $M \in S_F$, 使得 $1+|z_1|+\cdots+|z_1|^n <_{R^2} M$.

设 $f(x)=(x-z_1)f_1(x)$, 其中 $f_1(x)=a_0'x^{n-1}+a_1'x^{n-2}+\cdots+a_{n-1}' \in R_0(\sqrt{-1})[x]$. 根据归纳法原理, 可假定: 存在某个正元素 $\delta_1 \in P$, 使得对于 $R_0(\sqrt{-1})[x]$ 中任意多项式 $g(x)=b_0x^{n-1}+b_1x^{n-2}+\cdots+b_{n-1}$, $g(x)$ 在 Ω 中恰有 m_1-1 个根 y, 满足 $|z_1-y| <_{R^2} c$, 同时恰有 m_j 个根 y, 满足 $|z_j-y| <_{R^2} c$, $j=2,\cdots,r$, 只要 $|b_i-a_i'| <_{R^2} \delta_1$, $i=0,1,\cdots,n-1$.

考虑 $R_0(\sqrt{-1})$ 上的如下诸多项式:

$$\begin{aligned} & h_i(x_0,\cdots,x_{n-1},y) \\ = \ & (a_0+x_0)(z_1+y)^i+(a_1+x_1)(z_1+y)^{i-1}+\cdots+(a_i+x_i), \end{aligned}$$

这里 $i=0,1,\cdots,n-1$.

易见, $h_i(0,\cdots,0,0)=a_i'$, $i=0,1,\cdots,n-1$. 由多项式函数的连续性知, 存在某个正元素 $\delta_2 \in P$, 使得对于任意 $\alpha_0,\cdots,\alpha_{n-1},\beta \in \Omega$, $|h_i(\alpha_0,\cdots,\alpha_{n-1},\beta)-a_i'| <_{R^2} \delta_1$, $i=0,1,\cdots,n-1$, 只要 $|\alpha_i| <_{R^2} \delta_2$, $i=0,1,\cdots,n-1$, 且 $|\beta| <_{R^2} \delta_2$.

令 $\delta=\min\{\delta_2, \frac{\delta_2^n|a_0|}{2M}, \frac{1}{2}|a_0|, \frac{c^n|a_0|}{2M}\}$, 且设 $g(x)=b_0x^n+b_1x^{n-1}+\cdots+b_n \in F[x]$, 使得 $|b_i-a_i| <_{R^2} \delta$, $i=0,1,\cdots,n$. 此时, $|b_0| \geqslant_{R^2} |a_0|-|b_0-a_0| >_{R^2} \frac{1}{2}|a_0| > 0$. 令 $y_1,\cdots,y_n$ 是 $g(x)$ 在 Ω 中的全部根, 则

$$\begin{aligned} |g(z_1)| &= |g(z_1)-f(z_1)| \\ &\leqslant_{R^2} |b_0-a_0||z_1|^n+|b_1-a_1||z_1|^{n-1}+\cdots+|b_n-a_n| \\ &<_{R^2} \delta M \leqslant_{R^2} \tfrac{c^n|a_0|}{2} <_{R^2} c^n|b_0|. \end{aligned}$$

由此有

$$|y_1-z_1|\cdots|y_n-z_1| <_{R^2} c^n.$$

同样有

$$|y_1-z_1|\cdots|y_n-z_1| <_{R^2} \delta_2^n.$$

从而有

$$|y_1-z_1|\cdots|y_n-z_1| <_{R^2} (\min\{c,\delta_2\})^n.$$

这表明: 必有某个 $k \in \{1,\cdots,n\}$, 使得 $|y_k-z_1| <_{R^2} \min\{c,\delta_2\}$. 不妨设 $|y_1-z_1| <_{R^2} \min\{c,\delta_2\}$.

令 $g(x)=(x-y_1)g_1(x)$, 这里 $g_1(x)=b_0'x^{n-1}+b_1'x^{n-2}+\cdots+b_{n-1}' \in R_0(\sqrt{-1})[x]$.

易见, $b'_i = h_i(b_0 - a_0, \cdots, b_{n-1} - a_{n-1}, y_1 - z_1)$, $i = 0, \cdots, n-1$. 注意到, $|y_1 - z_1| <_{R^2} \delta_2$, 且 $|b_i - a_i| <_{R^2} \delta_2, i = 0, 1, \cdots, n-1$. 从而 $|b'_i - a'_i| <_{R^2} \delta_1, i = 0, 1, \cdots, n-1$. 由上面的讨论知, $g_1(x)$ 在 Ω 中恰有 $m_1 - 1$ 个根 y, 满足 $|z_1 - y| <_{R^2} c$, 同时恰有 m_j 个根 y, 满足 $|z_j - y| <_{R^2} c, j = 2, \cdots, r$. 因此, 元素 δ 为所求. 证毕.

推论 设 (F, P) 是一个序域, R 是 F 的一个实闭扩张, 使得 $P \subseteq R^2$, 且正锥 R^2 在 F 上是阿基米德的. 若 $R[x]$ 中多项式 $f(x) = x^n + \beta_1 x^{n-1} + \cdots + \beta_n$ 在 R 中有单根 u, 则对于任意给定的正元素 $c \in P$, 必有某个正元素 $d \in P$, 使得只要 $F[x]$ 中多项式 $g(x) = x^n + b_1 x^{n-1} + \cdots + b_n$ 满足: $|b_i - \beta_i| <_{R^2} d, i = 1, \cdots, n$, $g(x)$ 在 R 中必有一个根 v, 且满足 $|u - v| <_{R^2} c$.

证明 设 $\Omega = R(\sqrt{-1})$, 且 $z_1 = u, \cdots, z_r$ 为 $f(x)$ 在 Ω 中全部相异的根. 不失一般性, 可设 $c <_{R^2} \min\{|z_i - z_j| \mid 1 \leqslant i < j \leqslant r\}$. 由引理 4.2.3 知, 有某个正元素 $\delta \in R^2$, 使得对于 $R[x]$ 中任意多项式 $g(x) = x^n + b_1 x^{n-1} + \cdots + b_n$, $g(x)$ 在 Ω 中恰有一个根 v, 满足 $|u - v| <_{R^2} c$, 只要 $|b_i - \beta_i| <_{R^2} \delta, i = 1, \cdots, n$. 由于正锥 R^2 在 F 上是阿基米德的, 从而有 P 中正元素 d, 使得 $d <_{R^2} \delta$. 这样, 对于 $F[x]$ 中任意多项式 $g(x) = x^n + b_1 x^{n-1} + \cdots + b_n$, $g(x)$ 在 Ω 中有惟一的根 v, 满足 $|u - v| <_{R^2} c$, 只要 $|b_i - \beta_i| <_{R^2} d, i = 1, \cdots, n$.

假若 $v \notin R$, 则 $g(\bar{v}) = 0$, 这里 $\bar{v}$ 是 v 的 R- 共轭元. 此时, 显然 $|u - \bar{v}| = |u - v| <_{R^2} c$, 这矛盾于 v 的惟一性. 因而, $v \in R$. 这表明: 多项式 $g(x)$ 在 R 中有一个根 v, 满足 $|u - v| <_{R^2} c$. 证毕.

在上面结论的基础上, 可建立下面的重要定理. 这一定理说明, 要使得序域 (F, P) 上的半正定多项式能表作有理函数的平方和, 条件 "F 在 (F, P) 的实闭包中稠密" 也是必要的.

定理 4.2.4 (McKenna) 序域 (F, P) 具有弱 Hilbert 性质, 当且仅当 F 在它关于 P 的实闭包 R 内是稠密的.

证明 定理的充分性可从定理 4.1.2 直接得出, 下证必要性.

用 $\widetilde{F}$ 表示由 R 中全体关于 F 的极限元所组成的子域. 假若 F 在 R 内不是稠密的, 则 R 中必有关于 F 的孤立元, 令 α 是 R 中一个关于 F 的孤立元, 且令 $p(x)$ 是 α 在 F 上的极小多项式. 我们可以选择这样一个孤立元 α, 使得其极小多项式 $p(x)$ 有最小的次数 m. 显然, $m > 1$. 如果 $p(x)$ 在 R 中尚有其他的根: $\alpha_2, \cdots, \alpha_r$, 则可断言: $\alpha_2, \cdots, \alpha_r$ 都是关于 F 的孤立元. 因若不然, 可设 α_2 是极限元, 则有 $p_1(x) \in \widetilde{F}[x]$, 使得 $p(x) = (x - \alpha_2)p_1(x)$. 由于 α 是 R 中关于 F 的孤立元, 则对于某个正元素 $c \in P$, R 中开区间 $]\alpha - c, \alpha + c[_{R^2}$ 不包含 F 的元素. 由定理 1.4.2 知, 正锥 R^2 在 F 上是阿基米德的. 注意到, F 在 $\widetilde{F}$ 中是稠密的, $p_1(x)$ 是 $\widetilde{F}$ 上一个 $m-1$ 次的多项式, 且 α 为其单根. 根据引理 4.2.3 的推论, F 上有一个次数为

$m-1$ 的多项式，它有一个根 β，使得 $|\alpha-\beta|<_{R^2}\frac{c}{2}$. 此时，开区间 $]\beta-\frac{c}{2},\beta+\frac{c}{2}[_{R^2}$ 不包含 F 的元素. 从而 β 也是关于 F 的孤立元，但这与 α 的取法矛盾. 因此，$\alpha_2,\cdots,\alpha_r$ 都是关于 F 的孤立元.

现在我们来作出一个在 (F,P) 上是半正定的，但不是强半正定的单元多项式. 对于上面出现的每个根 α_i，都有一个 R 中开区间 $]\alpha_i-c_i,\alpha_i+c_i[_{R^2}$ 不包含 F 的元素，其中 $c_i\in P, i=1,\cdots,r$. 取 $c=\min\{c_i\mid i=1,\cdots,r\}$，于是 $\alpha_i+\frac{c}{2}$ 是孤立元，$i=1,\cdots,r$. 令 $q(x)=p(x-\frac{c}{2})$，则 $q(x)$ 是 F 上的多项式，且 $\alpha_1+\frac{c}{2},\cdots,\alpha_r+\frac{c}{2}$ 为它在 R 中的全部根.

再令 $f(x)=p(x)q(x)$. 现证明：$f(x)$ 在 F 上是半正定的，但不是强半正定的. 假若对于某个 $a\in F$, $f(a)<_P 0$ 即 $p(a)p(a-\frac{c}{2})<_P 0$，则由中间值定理知，$p(x)$ 在 R 内有根 β，使得 $a-\frac{c}{2}<_{R^2}\beta<_{R^2}a$. 此时必有 $\beta=\alpha_j$, $1\leqslant j\leqslant r$. 从而 $a-\frac{c}{2}<_{R^2}\alpha_j<_{R^2}a$，即 $\alpha_j<_{R^2}a<_{R^2}\alpha_j+\frac{c}{2}$，与 c 的取法矛盾. 因而，$f(x)$ 在 (F,P) 上是半正定的. 另一方面，若 $\alpha_k=\max\{\alpha_i\mid i=1,\cdots,r\}$, $1\leqslant k\leqslant r$，则 $\alpha_k+\frac{c}{2}$ 是 $f(x)$ 的 (最大) 单根. 从而当 x 通过 $\alpha_k+\frac{c}{2}$ 时，$f(x)$ 必变号. 因此，$f(x)$ 在 R 上不是半正定的，即 $f(x)$ 在 (F,P) 上不是强半正定的. 由命题 4.2.1 知，序域 (F,P) 不具有弱 Hilbert 性质. 必要性证毕.

下面的推论可直接从上面定理的证明中得出.

推论 序域 (F,P) 有弱 Hilbert 性质，当且仅当 (F,P) 上每个半正定的单元多项式都是强半正定的.

结合命题 4.2.1 和定理 4.2.4, 立即可获得下面结果.

定理 4.2.5 序域 (F,P) 具有 Hilbert 性质，当且仅当 F 在它关于 P 的实闭包 R 内是稠密的，且 $P=S_F$，即 P 是域 F 惟一的序.

推论 序域 (F,P) 具有 Hilbert 性质，当且仅当 (F,P) 上每个半正定的单元多项式都能表为单元有理函数的平方和.

在后面，我们将看到，上面推论中的"单元有理函数"一词尚可改进为"单元多项式".

§4.3 仅有有限个序且具有弱 Hilbert 性质的亚序域

在 §4.2 中，我们就序域的情形讨论了 Hilbert 第十七问题的逆问题. 在本节和下一节，我们将对亚序域的情形进行讨论. 在本节中，只讨论仅有有限个序的亚序域. 至于一般情形，则留待于下一节讨论. 从命题 4.2.1 可见，对于亚序域 (F,T) 而言，Hilbert 性质与弱 Hilbert 性质的差异，仅仅在于是否有 $T=S_F$. 因此，下面的讨论不妨仅针对弱 Hilbert 性质.

序域可以看作是仅有一个序的亚序域. 因此，McKenna 定理可看作对仅有一

个序且具有弱 Hilbert 性质的亚序域的一个刻画. 作为 McKenna 定理的一个推广, 可建立如下定理.

定理 4.3.1 设 (F,T) 是一个仅有有限个序的亚序域, 则 (F,T) 具有弱 Hilbert 性质, 当且仅当 F 在 (F,T) 的每个实闭包中都是稠密的.

证明 充分性: 按定理 4.1.3, 只须证明: 亚序域 (F,T) 上的每个非强半正定的多项式, 同时也不是半正定的. 设多项式 $f(x_1,\cdots,x_n)$ 在 (F,T) 上不是强半正定的, 即对于 (F,T) 的某个实闭包 R 以及某些 $\alpha_1,\cdots,\alpha_n\in R$, 有 $f(\alpha_1,\cdots,\alpha_n)<_{R^2}0$. 由多项式函数的连续性以及 F 在 R 中的稠密性知, 有 $a_1,\cdots,a_n\in F$, 使得 $f(a_1,\cdots,a_n)<_P 0$, 此处 $P:=R^2\cap F$ 是亚序域 (F,T) 的一个序. 因此, $f(x_1,\cdots,x_n)$ 在 (F,T) 上也不是半正定的.

必要性: 设 $P, P_1,\cdots,P_m$ 是亚序域 (F,T) 的所有的相异正锥, 且以 R 表示 F 关于序 P 的实闭包. 由于 $P\not\subseteq P_i$, 从而有 $a_i\in P\setminus P_i$, $i=1,\cdots,m$. 今证明, F 在 R 中稠密.

假若断言不成立, 则 R 中必有关于 F 的孤立元, 即有某个 $\alpha\in R$ 以及某个正元素 $c\in P$, 使得 $]\alpha-c,\alpha+c[_{R^2}$ 与 F 是分离的. 设 α 在 F 上的极小多项 $f(x)$ 在 $R[x]$ 中分解成

$$\begin{aligned}f(x) &= (x-\alpha_1)\cdots(x-\alpha_r)(x-\beta_1)\cdots(x-\beta_s)\\ &\quad [(x-u_1)^2+v_1^2]\cdots[(x-u_t)^2+v_t^2],\end{aligned}$$

其中 $\alpha_1=\alpha$, α_i, β_j, u_k, $v_k\in R$, $v_k\neq 0$, 且 $]\alpha_i-\frac{c}{2},\alpha_i+\frac{c}{2}[_{R^2}$ 与 F 是分离的, 但 $]\beta_j-\frac{c}{2},\beta_j+\frac{c}{2}[_{R^2}$ 则否, $i=1,\cdots,r$; $j=1,\cdots,s$; $k=1,\cdots,t$.

于是存在 $b_j\in F$, 满足 $|b_j-\beta_j|<_{R^2}\frac{c}{2}$, $j=1,\cdots,s$. 此外, 由于 v_k 是 F 上的非零代数元, 则由引理 1.2.2 可知, 有正元素 $c_k\in P$, 使得 $|v_k|>c_k$, $k=1,\cdots,t$.

令 $\Delta=(\frac{c}{2})^{r+s}c_1^2\cdots c_t^2$. 考虑如下多项式:

$$H(x;y_i;z_j)=\Delta^{-2}f^2(x)-1+\sum_{i=1}^{s}\{y_i^2[(x-b_i)^2-c^2]-1\}^2+\sum_{j=1}^{m}(a_jz_j^2-1)^2.$$

显然, $H(x;y_i;z_j)$ 是 F 上的一个 $s+m+1$ 元多项式, 且当 $x=\alpha\in R$, $y_i=(\sqrt{(\alpha-b_i)^2-c^2})^{-1}\in R$, $i=1,\cdots,s$, 且 $z_j=(\sqrt{a_j})^{-1}\in R$, $j=1,\cdots,m$, 多项式 $H(x;y_i;z_j)$ 所取的值为 -1. 因此, 多项式 $H(x;y_i;z_j)$ 在 (F,T) 上不是强半正定的. 由于 (F,T) 具有弱 Hilbert 性质, 从而根据命题 4.2.1, 多项式 $H(x;y_i;z_j)$ 在 (F,T) 上也不是半正定的. 这意味着: 对于 $\{P,P_1,\cdots,P_m\}$ 中的某个 P_0, 以及 F 中元素 a, $d_1,\cdots,d_s$, $e_1,\cdots,e_m$, 有

$$H(a;d_i;e_j)<_{P_0}0,$$

即下式成立:

$$\Delta^{-2}f^2(a)-1+\sum_{i=1}^{s}\{d_i^2[(a-b_i)^2-c^2]-1\}^2+\sum_{j=1}^{m}(a_je_j^2-1)^2<_{P_0}0.$$

由此可得

$$\begin{gathered}\Delta^{-2}f^2(a)<_{P_0}1;\\ d_i^2[(a-b_i)^2-c^2]>_{P_0}0;\ i=1,\cdots,s;\\ a_je_j^2>_{P_0}0;\ j=1,\cdots,m.\end{gathered}$$

于是有 $a_j>_{P_0}0$, 即 $a_j\in P_0$, $j=1,\cdots,m$. 从 $a_1,\cdots,a_m$ 的取法, 我们有 $P_0=P$. 从而有

$$f^2(a)<_P\Delta^2, \qquad (\star)$$

以及 $(a-b_i)^2>_P c^2$ 即 $|a-b_i|>_P c$, $i=1,\cdots,s$. 于是, $|a-\beta_i|>_{R^2}|a-b_i|-|b_i-\beta_i|>_{R^2}c-\dfrac{c}{2}=\dfrac{c}{2}$, $i=1,\cdots,s$.

由于 $]\alpha_i-\dfrac{c}{2},\alpha_i+\dfrac{c}{2}[_{R^2}$ 与 F 是分离的, 故有 $|\alpha_i-a|>_{R^2}\dfrac{c}{2}$, $i=1,\cdots,r$. 于是又有

$$\begin{aligned}f^2(a)&=(a-\alpha_1)^2\cdots(a-\alpha_r)^2(a-\beta_1)^2\cdots(a-\beta_s)^2\\ &\quad[(a-u_1)^2+v_1^2]^2\cdots[(a-u_t)^2+v_t^2]^2\\ &>_{R^2}\left(\frac{c}{2}\right)^{2r+2s}c_1^4\cdots c_t^4=\Delta^2,\end{aligned}$$

与上式 $(\star)$ 矛盾. 必要性即告证明.

由定理 4.3.1, 立即可推出 A. Prestel 所建立的如下结果.

定理 4.3.2 设 F 是一个仅有有限个序的实域, 则 (F,S_F) 具有 Hilbert 性质, 当且仅当 F 在它的每个实闭包中都是稠密的.

由上述定理, 人们也许会猜测: 对于任何一个有弱 Hilbert 性质的亚序域 (F,T), F 在 (F,T) 的每个实闭包内都是稠密的. 但事实并不如此, 请看下例:

例 设 $F=\mathbb{R}(t)$, 其中 t 是实数域 $\mathbb{R}$ 上的一个未定元, 记 T 为域 F 的弱亚正锥 $S_{\mathbb{R}(t)}$. 下面将考虑亚序域 (F,T). 对此, 可证明以下的论断:

(1) 亚序域 (F,T) 具有 Hilbert 性质. 按命题 4.2.1, 只须证明亚序域 (F,T) 具有弱 Hilbert 性质, 即 (F,T) 上每个非强半正定多项式同时也不是半正定的.

设 $f(x_1,\cdots,x_n)$ 是 (F,T) 上一个非强半正定多项式, 则对于 (F,T) 的某个实闭包 R 以及某些 $\alpha_1,\cdots,\alpha_n\in R$, 有 $f(\alpha_1,\cdots,\alpha_n)<_{R^2}0$.

取非零 $d(t)\in\mathbb{R}[t]$, 使得 $d^2(t)f(x_1,\cdots,x_n)\in\mathbb{R}[t,x_1,\cdots,x_n]$. 此时有

$$g(t,\alpha_1,\cdots,\alpha_n)<_{R^2}0,$$

其中 $g(t,x_1,\cdots,x_n):=d^2(t)f(x_1,\cdots,x_n)\in\mathbb{R}[t,x_1,\cdots,x_n]$.

由定理 3.6.7 知，存在一个从 $\mathbb{R}[t,\alpha_1,\cdots,\alpha_n]$ 到 $\mathbb{R}$ 的 $\mathbb{R}$- 代数同态 ϕ, 使得

$$\phi(g(t,\alpha_1,\cdots,\alpha_n))<0,\ 即\ g(c,a_1,\cdots,a_n)<0,$$

其中 $c=\phi(t)$, $a_i=\phi(\alpha_i)$, $i=1,\cdots,n$.

根据定理 2.6.3, 我们可规定 $\mathbb{R}(t)$ 的一个正锥 P, 使得 $t-c$ 关于 P 是在 $\mathbb{R}$ 上的无限小元素. 由多项式函数的连续性知，从上式可得

$$g(t,a_1,\cdots,a_n)=g(c+(t-c),a_1,\cdots,a_n)<_P 0.$$

从而有

$$f(a_1,\cdots,a_n)=g(t,a_1,\cdots,a_n)d^{-2}(t)<_P 0.$$

这表明： $f(x_1,\cdots,x_n)$ 在 (F,T) (即 $(\mathbb{R}(t),S_{\mathbb{R}(t)})$) 上不是半正定的.

(2)F 在 (F,T) 的每个实闭包中都不是稠密的. 设 R 是 (F,T) 的任意一个实闭包. 令 $P=R^2\cap F$. 不失一般性，可设 $t\in P$. 今证明， F 中有一个 e, 使得 $F=\mathbb{R}(e)$, 且 e 关于 P 是在 $\mathbb{R}$ 上的正无限小元素.

若 t 是在 $\mathbb{R}$ 上的正无限大元素，则取 $e=t^{-1}$ 即可. 否则，必有某个 $a\in\mathbb{R}$, 使得 $t<_P a$. 此时实数集

$$M=\{r\in\mathbb{R}\mid t<_P r\}$$

是一个有下界 0 的非空集，从而存在下确界 $c\in\mathbb{R}$. 此时可断言： $|t-c|$ 是在 $\mathbb{R}$ 上的正无限小元素. 事实上，对于任意正实数 $\epsilon\in\mathbb{R}$, $c-\epsilon\notin M$, 即有 $c-\epsilon<_P t$. 从而 $-\epsilon<_P t-c$. 另一方面，有 $r_0\in M$, 使得 $r_0<c+\epsilon$. 因此， $t-c<_P r_0-c<_P\epsilon$. 从而 $|t-c|<_P\epsilon$. 于是， $e=|t-c|$ 满足如上要求.

依照 §4.1 中的例子，可以证明： R 中开区间 $]\sqrt{e},2\sqrt{e}[_{R^2}$ 与 $F\ (=\mathbb{R}(e))$ 是分离的.

§4.4 亚序域的局部稠密性与弱 Hilbert 性质

上节末的例子说明了这样一个事实：对于亚序域， “稠密性” 一般来说是一个强于 “弱 Hilbert 性质” 的概念. 因此，自然会产生这样一个问题：怎样给出一个与 “弱 Hilbert 性质” 等价的特性，使得这一特性与稠密性具有相近的性质和一定的关

联？这就是本节所要讨论的中心问题.

定义 4.4.1 一个亚序域 (F,T) 称作是局部稠密的，如果对于 (F,T) 的每个有限实扩张 K 以及任何相异的 $\alpha,\beta\in K$, 总有一个 $a\in F$, 使得对于 K 的某个包含 T 的正锥 Q, 有 $a\in]\alpha,\beta[_Q$, 这里及以后各处， $]\alpha,\beta[_Q$ 表示 K 中关于 Q 的且以 α 和 β 为端点的开区间，并不意指 $\alpha<_Q\beta$.

以下始终设 F 是一个实域， Ω 是 F 的代数闭包. 不失一般性，可以认定 F 的任何代数扩张都包含在 Ω 之内. 设 R 是 F 的任何一个实闭包. 按定理 2.1.3, 有 $\Omega=R(\sqrt{-1})$. 从而对于 Ω 中每个元素 z, 可惟一地写为： $z=a+b\sqrt{-1}$, 其中 a,b 都属于 R. 此时，称 b 为 z 关于 R 的虚部系数，且记作： $b=\mathrm{Im}_R(z)$. 同时，我们还可规定 z 关于正锥 R^2 的绝对值 $|z|_{R^2}$ 如下：

$$|z|_{R^2}=\sqrt{a^2+b^2}\in R,$$

这里 $\sqrt{a^2+b^2}$ 表示多项式 $x^2-(a^2+b^2)$ 在 R 中惟一的非负根.

容易验证，如上规定的 $|\cdot|_{R^2}$ 具有和通常复数的绝对值相类似的性质. 为简便起见，在不引起误解的情况下，记号 $|\cdot|_{R^2}$ 常简写为 $|\cdot|$.

在建立主要结果之前，首先给出下面几个引理.

引理 4.4.1 设 $f(x)$ 是 F 上一个次数 >0 的多项式，则有 $e,M\in S_F$, 使得对于 F 的每个实闭包 R, 总有

$$e<_{R^2}|\alpha|_{R^2}<_{R^2}M,$$

此处 α 是 $f(x)$ 在 Ω 中的任何一个非零根.

证明 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$，其中 $a_0\neq 0,\ n\geqslant 1$. 令 $M=\frac{1}{2}[n+1+(\frac{a_1}{a_0})^2+\cdots+(\frac{a_n}{a_0})^2]\in S_F$. 注意到，对于 F 的任意一个实闭包 R, 所规定的绝对值 $|\cdot|_{R^2}$ 具有和通常复数的绝对值相类似的性质. 从而通过引理 1.2.2 的类似证明可知，对于 $f(x)$ 在 Ω 中的任意一个根 α, 有 $|\alpha|_{R^2}<_{R^2}M$.

当 $\alpha\neq 0$ 时， α^{-1} 是 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$ 的根. 由上面的讨论知，有 $d\in S_F$, 使得 $|\alpha^{-1}|_{R^2}<_{R^2}d$. 因此，只须取 $e=d^{-1}$ 即可. 证毕.

引理 4.4.2 设 $f(x)$ 是 F 上的一个次数 >0 的多项式，则有 $e\in S_F$, 使得对于 F 的每个实闭包 R, 总有

$$|\mathrm{Im}_R(\alpha)|_{R^2}>_{R^2}e,$$

此处， α 是 $f(x)$ 在 Ω 中但不在 R 中的任意一个根.

证明 不失一般性，设 $f(x)$ 的首项系数为 1. 又设 Y,Z 是 F 上两个未定元，则有

$$f(Y+Z\sqrt{-1})=f_1(Y,Z)+f_2(Y,Z)\sqrt{-1},$$

其中 $f_1(Y,Z)$, $f_2(Y,Z)\in F[Y,Z]$. 此时可断言： $f_1(Y,Z)$ 与 $f_2(Y,Z)$ 无非常量的公因式.

假若 $d(Y,Z)$ 是 $f_1(Y,Z)$ 与 $f_2(Y,Z)$ 的一个非常量公因式，则有

$$f(Y+Z\sqrt{-1})=d(Y,Z)(q_1(Y,Z)+q_2(Y,Z)\sqrt{-1}),$$

此处 $q_1(Y,Z)$, $q_2(Y,Z)\in F[Y,Z]$.

设 $\alpha_1,\cdots,\alpha_n$ 是 $f(x)$ 在 Ω 内的全部根，其中 n 为多项式 $f(x)$ 的次数. 于是有

$$f(Y+Z\sqrt{-1})=(Y+Z\sqrt{-1}-\alpha_1)\cdots(Y+Z\sqrt{-1}-\alpha_n).$$

由于 $\Omega[Y,Z]$ 是惟一因式分解整环，故有

$$d(Y,Z)=b(Y+Z\sqrt{-1}-\alpha_{j_1})\cdots(Y+Z\sqrt{-1}-\alpha_{j_m}),\qquad(\star)$$

这里 $b\in F$, $j_1,\cdots,j_m$ 是取自 $1,\cdots,n$ 中的 m 个不同的数字.

设 R 是 F 的任意一个实闭包. 于是 $\Omega[Y,Z]=R[Y,Z][\sqrt{-1}]$. 令 τ 是环 $\Omega[Y,Z]$ 的一个 $R[Y,Z]$- 自同构，使得 $\tau(\sqrt{-1})=-\sqrt{-1}$. 于是有

$$d(Y,Z)=\tau(d(Y,Z))=b(Y-Z\sqrt{-1}-\tau(\alpha_{j_1}))\cdots(Y-Z\sqrt{-1}-\tau(\alpha_{j_m})).\qquad(\star\star)$$

这样就得到 $d(Y,Z)$ 在 $\Omega[Y,Z]$ 中的两个不相伴的因式分解 $(\star)$ 与 $(\star\star)$, 矛盾. 因而， $f_1(Y,Z)$ 与 $f_2(Y,Z)$ 无非常量的公因式.

记 $\mathrm{Res}(f_1,f_2;Y)$ 为多项式 $f_1(Y,Z)$ 与 $f_2(Y,Z)$ 关于未定元 Y 的结式，则 $\mathrm{Res}(f_1,f_2;Y)$ 是一个 F 上含未定元 Z 的正次数多项式. 由引理 4.4.1, 存在某个 $e\in S_F$, 使得对于 F 的每个实闭包 R, 总有

$$|\beta|_{R^2}>_{R^2}e,$$

此处 β 是 $\mathrm{Res}(f_1,f_2;Y)$ 在 Ω 中的任何一个非零根. 若 α 是 $f(x)$ 在 Ω 中但不在 R 中的任意一个根，则 $\mathrm{Im}_R(\alpha)$ 显然是 $\mathrm{Res}(f_1,f_2;Y)$ 的一个非零根. 由上面的论断，即有 $|\mathrm{Im}_R(\alpha)|_{R^2}>_{R^2}e$. 证毕.

引理 4.4.3　设 $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$, 且 $\alpha_1,\cdots,\alpha_n$ 是 Ω 中元素，使得 $f(\alpha_1,\cdots,\alpha_n)\neq 0$, 则存在一个 $d\in S_F$, 使得对于 F 的每个包含 $\alpha_1,\cdots,\alpha_n$ 的实闭包 R 以及任意 $y_1,\cdots,y_n\in R$, 只要 $|y_i-\alpha_i|_{R^2}<_{R^2}d$, $i=1,\cdots,n$, 总有

$$f(y_1,\cdots,y_n)f(\alpha_1,\cdots,\alpha_n)>_{R^2}0.$$

证明 在 F 的每个包含 $\alpha_1, \cdots, \alpha_n$ 的实闭包 R 中，由 Taylor 展开式，我们有如下的估计：

$$\begin{aligned} f(\overline{\alpha}+\overline{x})f(\overline{\alpha}): &= f(\alpha_1+x_1,\cdots,\alpha_n+x_n)f(\alpha_1,\cdots,\alpha_n) \\ &= f(\overline{\alpha})[f(\overline{\alpha})+\sum_{i_1\cdots i_n} f_{i_1\cdots i_n}(\overline{\alpha})x_1^{i_1}\cdots x_n^{i_n}] \\ &= f^2(\overline{\alpha})+\sum_{i_1\cdots i_n} f(\overline{\alpha})f_{i_1\cdots i_n}(\overline{\alpha})x_1^{i_1}\cdots x_n^{i_n} \\ &>_{R^2} f^2(\overline{\alpha})-\sum_{i_1\cdots i_n}[f^2(\overline{\alpha})+f^2_{i_1\cdots i_n}(\overline{\alpha})]|x_1|_{R^2}^{i_1}\cdots|x_n|_{R^2}^{i_n}. \end{aligned}$$

从而当 $|x_i|_{R^2} <_{R^2} 1, i=1, \cdots, n$, 我们有

$$f(\overline{\alpha}+\overline{x})f(\overline{\alpha}) >_{R^2} f^2(\overline{\alpha})-\sum_{i_1\cdots i_n}[f^2(\overline{\alpha})+f^2_{i_1\cdots i_n}(\overline{\alpha})](|x_1|_{R^2}+\cdots+|x_n|_{R^2}).$$

令 $\Delta=\frac{1}{n}f^2(\overline{\alpha})\{\sum\limits_{i_1\cdots i_n}[f^2(\overline{\alpha})+f^2_{i_1\cdots i_n}(\overline{\alpha})]\}^{-1}$, 则 $0 <_{R^2} \Delta <_{R^2} 1$, 且当 $|x_i|_{R^2} <_{R^2} \Delta, i=1,\cdots,n$, 有 $f(\overline{\alpha}+\overline{x})f(\overline{\alpha}) >_{R^2} 0$.

再按引理 4.4.1, 存在 $d\in S_F$, 使得有 $\Delta=|\Delta|_{R^2} >_{R^2} d$. 显然，这个 d 满足引理的要求. 证毕.

由如上引理，我们可以给出与局部稠密性等价的几个性质.

定理 4.4.4 对于一个亚序域 (F,T), 以下的断言是等价的：

(1) (F,T) 是局部稠密的;

(2) 对于 (F,T) 的每个有限实扩张 $F(\alpha)$ 以及每个非零 $e\in T$, $F(\alpha)$ 必有一个包含 T 的正锥 Q, 且有 $a\in F$, 使得 $|a-\alpha|_Q <_Q e$;

(3) 若 K 是 (F,T) 的一个有限实扩张，$\alpha_1,\cdots,\alpha_n\in K$, 且 e 为 T 中非零元，则 K 必有一个包含 T 的正锥 Q, 且有 $a_1,\cdots,a_n\in F$, 使得 $|a_i-\alpha_i|_Q <_Q e$, $i=1,\cdots,n$;

(4) 若 K 是 (F,T) 的一个有限实扩张，$\alpha_1,\cdots,\alpha_n,\beta_1,\cdots,\beta_n\in K$, 其中 $\alpha_i\neq\beta_i$, $i=1,\cdots,n$, 则 K 必有一个包含 T 的正锥 Q, 且有 $a_1,\cdots,a_n\in F$, 使得 $a_i\in]\alpha_i,\beta_i[_Q$, $i=1,\cdots,n$.

证明 (1) $\Longrightarrow$ (2): 由局部稠密性，有 $a\in F$, 使得对于 $F(\alpha)$ 的某个包含 T 的正锥 Q, 有 $a\in]\alpha-e,\alpha+e[_Q$, 即 $|a-\alpha|_Q <_Q e$.

(2) $\Longrightarrow$ (3): 由熟知的本原元定理，可设 $K=F(\alpha)$. 从而 $\alpha_i=h_i(\alpha)$, 此处 $h_i(x)\in F[x]$, $i=1,\cdots,n$. 考察多项式 $\psi(x,y)=\sum\limits_{i=1}^{n}(h_i(x)-h_i(y))^2-e^2$. 按引理 4.4.3 知，有非零 $d\in S_F$, 使得对于 F 的每个包含 α 的实闭包 R, 只要 $|x-\alpha|_{R^2} <_{R^2} d$ 且 $|y-\alpha|_{R^2} <_{R^2} d$, $\psi(x,y)$ 恒与 $\psi(\alpha,\alpha)=-e^2$ 同号，即 $\psi(x,y) <_{R^2} 0$. 由断言

(2) 知，有 $a \in F$, 使得对于 K 上的某个包含 T 的正锥 Q, $|a-\alpha|_Q <_Q d$. 从而 $\psi(a,\alpha) <_Q 0$, 即有

$$\sum_{i=1}^{n}(h_i(a)-\alpha_i)^2 = \sum_{i=1}^{n}(h_i(a)-h_i(\alpha))^2 <_Q e^2.$$

于是 $|h_i(a)-\alpha_i|_Q <_Q e, i=1,\cdots,n$. 令 $a_i = h_i(a), i=1,\cdots,n$, 则 $a_1,\cdots,a_n$ 即为所求.

(3) $\Longrightarrow$ (4): 由引理 4.4.1 知，有非零 $e_i \in S_F$, 使得对于 F 的每个实闭包 R, 恒有 $|\frac{\alpha_i-\beta_i}{2}|_{R^2} >_{R^2} e_i, i=1,\cdots,n$. 令 $e=\prod\limits_{i=1}^{n} e_i(1+e_i)^{-1} \in S_F$. 由断言 (3) 知，有 $a_1,\cdots,a_n \in F$, 使得对于 K 的某个包含 T 的正锥 Q, 有

$$|a_i - \tfrac{\alpha_i+\beta_i}{2}|_Q <_Q e, i=1,\cdots,n.$$

此时显然有

$$|a_i - \tfrac{\alpha_i+\beta_i}{2}|_Q <_Q e_i <_Q |\tfrac{\alpha_i-\beta_i}{2}|_Q, i=1,\cdots,n.$$

这表明： $a_i \in]\alpha_i,\beta_i[_Q, i=1,\cdots,n$.

(4) $\Longrightarrow$ (1): 显然成立. 证毕.

下面，我们来给出具有弱 Hilbert 性质的亚序域的一个刻画.

定理 4.4.5　亚序域 (F,T) 具有弱 Hilbert 性质，当且仅当 (F,T) 是局部稠密的.

证明　充分性：由命题 4.2.1, 只须证明每个在 (F,T) 上为非强半正定的多项式 $f(x_1,\cdots,x_n)$ 也不是半正定的. 根据非强半正定的所设，对于 (F,T) 的某个实闭包 R, 有 $\alpha_1,\cdots,\alpha_n \in R$, 使得 $f(\alpha_1,\cdots,\alpha_n) <_{R^2} 0$. 设 $d \in S_F$ 是由 $f(x_1,\cdots,x_n)$ 以及 $\alpha_1,\cdots,\alpha_n$ 所确定的，且满足引理 4.4.3 中结论的全正元素. 令 $K = F(\alpha_1,\cdots,\alpha_n,\sqrt{-f(\alpha_1,\cdots,\alpha_n)}) \subseteq R$, 于是 K 是亚序域 (F,T) 的一个有限实扩张. 由定理 4.4.4 中蕴含关系 "(1) $\Longrightarrow$ (3)" 知，有 K 的一个包含 T 的正锥 Q, 且有 $a_1,\cdots,a_n \in F$, 使得 $|a_i-\alpha_i|_Q <_Q d, i=1,\cdots,n$. 按引理 4.4.3, $f(a_1,\cdots,a_n)$ 与 $f(\alpha_1,\cdots,\alpha_n)$ 关于正锥 Q 有相同的符号. 由于 $f(\alpha_1,\cdots,\alpha_n) = -(\sqrt{-f(\alpha_1,\cdots,\alpha_n)})^2 <_Q 0$, 从而 $f(a_1,\cdots,a_n) <_Q 0$. 注意到， $Q\cap F$ 是 (F,T) 的一个正锥. 因此， $f(x_1,\cdots,x_n)$ 在 (F,T) 上不是半正定的.

必要性：根据定理 4.4.4 中蕴含关系 "(1) $\Longleftrightarrow$ (2)" 知，只须证明：对于 (F,T) 的每个有限实扩张 $F(\alpha)$ 以及非零 $e \in T$, 必有 K 的一个包含 T 的正锥 Q 以及某个 $a \in F$, 使得 $|a-\alpha|_Q <_Q e$.

设 $f(x)$ 是 α 在 F 上的极小多项式， e_1 是由 $f(x)$ 所确定的，且满足引理 4.4.2 的全正元素. 令 $\delta = ee_1(1+e)^{-1}(1+e_1)^{-1}$. 现考虑 F 上多项式 $\psi(x) = f^2(x) - \delta^{2n}$,

此处 n 是 $f(x)$ 的次数. 由于 $F(\alpha)$ 是 (F,T) 的一个实扩张, 从而 K 有一个包含 T 的正锥 Q_1. 此时有, $\psi(\alpha)=-\delta^{2n}<_{Q_1}0$. 因此, $\psi(x)$ 在 (F,T) 上不是强半正定的. 按所设, (F,T) 具有弱 Hilbert 性质. 由命题 4.2.1, $\psi(x)$ 在 (F,T) 上也不是半正定的. 于是, 对于 (F,T) 的某个正锥 P 以及某个 $a\in F$, 有 $\psi(a)<_P 0$, 即 $f^2(a)-\delta^{2n}<_P 0$. 从而有 $|f(a)|_P<_P\delta^n$.

设 R 是序域 (F,P) 的实闭包, 且 $f(x)$ 在 R 上可以分解为

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_r)[(x-u_1)^2+v_1^2]\cdots[(x-u_s)^2+v_s^2],$$

其中 $r+2s=n$, α_i, u_j, $v_j\in R$, 且 $v_j\neq 0$, $i=1,\cdots,r$; $j=1,\cdots,s$.

由前面不等式 $|f(a)|_P<_P\delta^n$, 可得

$$|(a-\alpha_1)\cdots(a-\alpha_r)|_{R^2}[(a-u_1)^2+v_1^2]\cdots[(a-u_s)^2+v_s^2]<_{R^2}\delta^n.$$

另一方面, 由引理 4.4.2 有

$$[(a-u_1)^2+v_1^2]\cdots[(a-u_s)^2+v_s^2]\geqslant_{R^2}v_1^2\cdots v_s^2>_{R^2}e_1^2\cdots e_1^2>_{R^2}\delta^{2s}.$$

这表明: $n>2s$, 因此 $r>0$. 从上面两式, 进一步可得到

$$|(a-\alpha_1)\cdots(a-\alpha_r)|_{R^2}<_{R^2}\delta^r.$$

因此, $\alpha_1,\cdots,\alpha_r$ 之中必有一个, 设为 α_1, 使得 $|a-\alpha_1|_{R^2}<_{R^2}\delta$.

记 π 是 $F(\alpha)$ 到 R 内的一个 F- 嵌入, 使得 $\pi(\alpha)=\alpha_1$. 令 $Q=\pi^{-1}(R^2)$. 显然, Q 是 $F(\alpha)$ 的一个正锥, 使得 $T\subseteq Q$. 由于 $-\delta<_{R^2}a-\alpha_1=\pi(a-\alpha)<_{R^2}\delta$, 从而有 $-\delta<_Q a-\alpha<_Q\delta$, 即 $|a-\alpha|_Q<_Q\delta<_Q e$. 必要性即告证明.

在上述必要性的证明过程中, 实际上只用到这样的一个事实: 每个在 (F,T) 上的半正定单元多项式也是强半正定的. 因此, 根据定理 4.4.5 的证明, 实际上可获得以下结论.

推论 1 亚序域 (F,T) 具有弱 Hilbert 性质, 当且仅当每个在 (F,T) 上的半正定单元多项式, 同时也是强半正定的.

推论 2 亚序域 (F,T) 具有 Hilbert 性质, 当且仅当每个在 (F,T) 上的半正定单元多项式都能表为单元有理函数的平方和.

为了阐明局部稠密性与稠密性之间的联系, 由定理 4.4.5 可以建立下面结果:

定理 4.4.6 设亚序域 (F,T) 具有弱 Hilbert 性质, 且 $P\in\mathcal{X}_F(T)$ 对于 Harrison 拓扑是一个孤立点, 则 F 在序域 (F,P) 的实闭包中稠密.

证明 设 R 是序域 (F,P) 的实闭包. 只需证明: 对于任意 $\alpha\in R$ 以及非零 $e\in P$, 存在一个 $a\in F$, 使得 $|a-\alpha|_{R^2}<_{R^2}e$.

设 $\alpha_1=\alpha$, $\cdots$, α_r 是 α 在 R 中全部 F- 共轭元. 由于 $P\in\mathcal{X}_F(T)$ 对于

Harrison 拓扑是一个孤立点，从而有 $\mathcal{X}_F(T)$ 的一个基本开子集 $H(b_1,\cdots,b_n)$，使得 $H(b_1,\cdots,b_n)=\{P\}$. 令 $K=F(\alpha_1,\cdots,\alpha_r,\sqrt{b_1},\cdots,\sqrt{b_n})$，则 $K\subseteq R$，即 K 是 (F,T) 的一个有限实扩张. 由定理 4.4.5 知，(F,T) 是局部稠密的. 根据定理 4.4.4，K 有一个包含 T 的正锥 Q，且有 $a_1,\cdots,a_n\in F$，使得 $|a_i-\alpha_i|_Q<_Q\frac{e^2}{1+e^2}$，$i=1,\cdots,n$. 注意到，$b_j=(\sqrt{b_j})^2\in Q\cap F$，$i=1,\cdots,n$. 从而 $Q\cap F\in H(b_1,\cdots,b_n)=\{P\}$，即 $Q\cap F=P$. 于是，(K,Q) 是序域 (F,P) 的一个代数序扩张. 因而，存在 (K,Q) 到 R 的一个保序 F- 嵌入 π. 此时，必有某个 α_k，$1\leqslant k\leqslant r$，使得 $\pi(\alpha_k)=\alpha$. 由 $|a_k-\alpha_k|_Q<_Q e$ 知，$|\pi(a_k-\alpha_k)|_{R^2}<_{R^2}\pi(e)$，即 $|a_k-\alpha|_{R^2}<_{R^2}e$. 因此，$F$ 在 R 中是稠密的. 证毕.

应用定理 4.4.6 很容易推出定理 4.3.1 的必要性 (自然也包括定理 4.3.2 和定理 4.2.4 的相同部分). 事实上，若亚序域 (F,T) 仅有有限个序，则 $\mathcal{X}_F(T)$ 中每个正锥都是孤立点，因为 $\mathcal{X}_F(T)$ 是一个有限的 Hausdorff 空间. 根据定理 4.4.6，F 在 (F,T) 的每个实闭包中稠密.

现使用定理 4.4.5 来证明下述命题，这一命题可看作 Hilbert 第十七问题的一个推广.

命题 4.4.7　设亚序域 (F,T) 具有弱 Hilbert 性质，$f,g_1,\cdots,g_s\in F[x_1,\cdots,x_n]$，其中 $g_1,\cdots,g_s$ 均非零. 若对于 (F,T) 的每个正锥 P 以及任意 $a_1,\cdots,a_n\in F$，只要 $g_i(a_1,\cdots,a_n)>_P 0$，$i=1,\cdots,s$，总有 $f(a_1,\cdots,a_n)\geqslant_P 0$，则 f 可以表成如下形式:

$$f=\sum_{i=1}^m t_i g_1^{k_{i1}}\cdots g_s^{k_{is}}h_i^2,$$

其中 m 为自然数，$t_i\in T$，$h_i\in F(x_1,\cdots,x_n)$，$k_{ij}=0$ 或 1，$i=1,\cdots,m$；$j=1,\cdots,s$.

证明　记 $K=F(x_1,\cdots,x_n)$，且作 K 的如下子集:

$$\widehat{T}:=\{\sum_{i=1}^m t_i g_1^{k_{i1}}\cdots g_s^{k_{is}}h_i^2\mid m>0,t_i\in T,h_i\in K,k_{ij}=0\text{ 或 }1,\ i=1,\cdots,m;\ j=1,\cdots,s\}.$$

假若命题不成立，即 $f\notin\widehat{T}$. 容易验知，此时 $\widehat{T}$ 是 K 的一个亚序. 按定理 1.1.2，K 有一个正锥 Q，使得 $f\notin Q$，以及 $\widehat{T}\subseteq Q$，注意到 $T\subseteq\widehat{T}\subseteq Q$，从而 $P=Q\cap F$ 是亚序域 (F,T) 的一个正锥. 令 R 是序域 (F,P) 的实闭包. 由于 $g_i\in\widehat{T}\subseteq Q$，$i=1,\cdots,s$，从而由定理 3.6.7 知，存在一个从 $F[x_1,\cdots,x_n]$ 到 R 的 F- 代数同态 ϕ，使

得有

$$\begin{cases} \phi(x_i)=\alpha_i\in R, & i=1,\cdots,n,\\ 0<_{R^2}\phi(g_j)\in R, & j=1,\cdots,s,\\ \phi(f)<_{R^2}0. \end{cases}$$

从而有

$$\begin{cases} g_j(\alpha_1,\cdots,\alpha_n) &=\phi(g_j)>_{R^2}0, j=1,\cdots,s,\\ f(\alpha_1,\cdots,\alpha_n) &=\phi(f)<_{R^2}0. \end{cases}$$

设 $d, d_1, \cdots, d_s$ 分别是由多项式 $f, g_1, \cdots, g_s$ 和元素 $\alpha_1, \cdots, \alpha_n$ 所确定的，且满足引理 4.4.3 的全正元素. 构造域 F 的如下扩张：

$$K=F(\alpha_1,\cdots,\alpha_n,\sqrt{g_1(\alpha_1,\cdots,\alpha_n)},\sqrt{g_s(\alpha_1,\cdots,\alpha_n)},\sqrt{-f(\alpha_1,\cdots,\alpha_n)}).$$

显然，$K\subseteq R$. 因而，K 是 (F,T) 的一个有限实扩张. 由定理 4.4.4 和 4.4.5, 有 K 的一个包含 T 的正锥 Q 以及 $a_1, \cdots, a_n\in F$, 使得

$$|a_i-\alpha_i|_Q<_Q\delta,\ i=1,\cdots,n,$$

这里 $\delta=d(1+d)^{-1}\prod_{j=1}^{s}d_j(1+d_j)^{-1}\in S_F$.

于是 $|a_i-\alpha_i|_Q<_Q\delta<_Q d_j$, $i=1,\cdots,n$; $j=1,\cdots,s$. 由引理 4.4.3, $g_j(a_1,\cdots,a_n)g_j(\alpha_1,\cdots,\alpha_n)>_Q 0$. 注意到，$g_j(\alpha_1,\cdots,\alpha_n)=(\sqrt{g_j(\alpha_1,\cdots,\alpha_n)})^2\in Q$, 即 $g_j(\alpha_1,\cdots,\alpha_n)>_Q 0$. 因此 $g_j(a_1,\cdots,a_n)>_Q 0$, $j=1,\cdots,s$. 同样，由于 $|a_i-\alpha_i|_Q<_Q d$, $i=1,\cdots,n$. 根据引理 4.4.3, 可得到 $f(a_1,\cdots,a_n)<_Q 0$. 令 $P=Q\cap F$, 则 P 是 (F,T) 的一个正锥，且有

$$\begin{aligned} g_j(a_1,\cdots,a_n)>_P 0, &\quad i=1,\cdots,s,\\ f(a_1,\cdots,a_n)<_P 0, & \end{aligned}$$

这与命题的所设矛盾. 因此应有 $f\in\widehat{T}$. 证毕.

§4.5 具有弱 Hilbert 性质的域的实赋值

在这一节中，我们研究具有弱 Hilbert 性质的序域与亚序域的实赋值，从赋值论角度进一步了解具有弱 Hilbert 性质的序域与亚序域.

首先，我们考虑具有弱 Hilbert 性质的序域. 由 McKenna 定理，我们容易建立如下事实：

命题 4.5.1 设 (F,P) 是一个序域，v 是 F 的一个与 P 相容的非浅显赋值. 若 (F,P) 具有弱 Hilbert 性质，则 v 的值群 G_v 是可除群，且剩余域 F_v 是实闭域.

证明　设 R 是序域 (F,P) 的实闭包. 由定理 3.2.5 知, v 可 (惟一地) 拓展为 R 的一个实赋值 w. 根据定理 3.4.10, 赋值 w 的值群 G_w 是一个可除群, 且剩余域 F_w 是一个实闭域. 为证明命题, 只须证明 $G_v = G_w$, 且 $F_v = F_w$.

显然, $G_v \subseteq G_w$, 且 $F_v \subseteq F_w$. 设 $h \in G_w$, 且 $h > 0$, 则有 $\alpha \in R$, 使得 $h = w(\alpha)$. 由定理 4.2.4 知, F 在 R 中是稠密的. 从而有 $a \in F$, 使得 $|a-\alpha|_{R^2} <_{R^2} \alpha^2$. 由于赋值 w 与 R 的惟一正锥 R^2 是相容的, 从而 $w(|a-\alpha|_{R^2}) \geqslant w(\alpha^2) = 2h > h$, 即 $w(a-\alpha) > w(\alpha)$. 由此有, $v(a) = w(a) = w((a-\alpha)+\alpha) = w(\alpha) = h$, 即有 $h = v(a) \in G_v$. 因而有 $G_v = G_w$.

再设 $\bar{\alpha} = \alpha + M_w \in F_w$, 其中 α 是 w 的赋值环 A_w 中元素, M_w 是 w 的赋值理想. 由于 v 是非浅显赋值, 从而有某个 $c \in F$, 使得 $v(c) > 0$. 不失一般性, 不妨设 $c >_P 0$. 由于 F 在 R 中稠密, 从而有 $a \in F$, 使得 $|a-\alpha|_{R^2} <_{R^2} c$. 由 w 与序 $\leqslant_{R^2}$ 的相容性知, $w(a-\alpha) \geqslant w(c) > 0$. 由此有 $a-\alpha \in M_w$, 即有 $a = (a-\alpha)+\alpha \in A_w$. 此时有 $\bar{\alpha} = \alpha + M_w = a + M_w = \bar{a} \in F_v$. 因而有, $F_v = F_w$. 证毕.

然而, 上面命题的逆形式不成立, 见下例.

例　设 $G = (\mathbb{Q},+)$ 是由有理数组成的加法群, 且 G 中元素间的序关系即为通常有理数之间的大小关系, 则 G 是一个可除的序群. 记 $G^2 = G \times G$, 则 G^2 也是一个可除序群, 其中元素之间的序关系 $\leqslant$ 为由 G 的序所确定的字典序, 即对于 (a,b), $(c,d) \in G^2$, $(a,b) < (c,d)$ 当且仅当 $a < c$, 或者 $a = c$ 但 $b < d$.

令 $\mathbb{R}[G^2]$ 是群 G^2 在实数域 $\mathbb{R}$ 上的群环, 则 $\mathbb{R}[G^2]$ 是一个整环. 对于任意非零 $z \in \mathbb{R}[G^2]$, z 可惟一表为

$$z = \alpha_1(a_1,b_1) + \cdots + \alpha_m(a_m,b_m),$$

其中 $\alpha_i \in \mathbb{R}$, $(a_i,b_i) \in G^2$, $i = 1, \cdots, m$, $\alpha_1 \neq 0$, 且 $(a_1,b_1) < (a_2,b_2) < \cdots < (a_m,b_m)$. 此时, α_1 称作元素 z 的尾项系数. 此外, 可规定 $v_0(z) = a_1$, 而 $w_0(z) = (a_1,b_1)$.

记 F 为 $\mathbb{R}[G^2]$ 的分式域. 对于任意非零 $\frac{z_1}{z_2} \in F$, 其中 z_1, $z_2 \in \mathbb{R}[G^2]$, 进一步规定 $v(\frac{z_1}{z_2}) = v_0(z_1) - v_0(z_2)$, 而 $w(\frac{z_1}{z_2}) = w_0(z_1) - w_0(z_2)$. 容易证明: 所规定的 v 和 w 都是域 F 的非浅显赋值.

令 P 是由 F 中零元以及所有这样的非零元 $\frac{z_1}{z_2}$ 组成的子集, 其中 z_1z_2 的尾项系数为正实数. 显然, P 是 F 的一个正锥. 容易验证: v 和 w 都与 P 相容.

不难知道, 赋值 w 的值群为 G^2, 其剩余域为 $\mathbb{R}$. 因此, w 的值群是可除群, 且剩余域是实闭域.

然而, 序域 (F,P) 不具有弱 Hilbert 性质. 事实上, 如若不然, 则由命题 4.5.1 知, v 的剩余域 F_v 是实闭域. 注意到, v 的剩余域 F_v 为群环 $\mathbb{R}[\{0\} \times G]$ 的分式域. 据此, 不难验证, $\pm[(0,0)+(0,1)]$ 都不是 F_v 中元素的平方, 矛盾.

然而，当命题 4.5.1 中的赋值 v 为一阶赋值时，命题 4.5.1 的逆也是成立的.

命题 4.5.2 设 (F,P) 是一个序域， v 是 F 的一个与 P 相容的一阶赋值，则 (F,P) 具有弱 Hilbert 性质，当且仅当 v 的值群是可除群，且其剩余域为实闭域.

证明 由命题 4.5.1 知，只需证明充分性. 由于 v 是一阶赋值，从而赋值域 (F,v) 有一个完备化 $(\widetilde{F},\widetilde{v})$. 由赋值论知， $\widetilde{v}$ 是域 $\widetilde{F}$ 的 Hensel 赋值. 由命题 3.4.2(1) 知， $(\widetilde{F},\widetilde{v})$ 包含 (F,v) 的一个 Hensel 化 (R,w)，其中 $F\subseteq R\subseteq\widetilde{F}$，$w$ 是 $\widetilde{v}$ 在 R 上的限制，即 $w=\widetilde{v}\mid_R$. 根据定理 3.4.4, w 是域 K 的一个实赋值. 由于 (R,w) 是 (F,v) 的直接扩张 (见命题 3.4.2(2))，从而由所设知， w 的值群是可除群，且其剩余域是实闭域. 再由定理 3.4.10 知， R 是一个实闭域. 由于 v 与 P 相容，从而由引理 3.4.6 知， P 可拓展为 R 的一个正锥，这个正锥只能是 R 的惟一正锥 R^2. 这表明： R 实际上是序域 (F,P) 的实闭包.

设 $\alpha\in R$, 且 e 为 P 中非零元，则 $\alpha\in\widetilde{F}$, 且 $v(e)\in G_v$. 由于 F 关于赋值 $\widetilde{v}$ 在 $\widetilde{F}$ 中是稠密的，从而有 $a\in F$, 使得 $\widetilde{v}(a-\alpha)>v(e)$, 即 $w(|a-\alpha|_{R^2})>w(e)$. 由定理 3.4.5 知， w 与 $\leqslant_{R^2}$ 是相容的. 从而必有 $|a-\alpha|_{R^2}<_{R^2}e$. 这表明： F 在实闭包 R 中稠密. 根据定理 4.2.4, (F,P) 具有弱 Hilbert 性质. 证毕.

为用赋值理论来刻画具有弱 Hilbert 性质的序域和亚序域，我们需要如下定义.

定义 4.5.1 设 K 是域 F 的一个扩张， W 是由域 K 的若干个赋值组成的集合. 称 F 和 K 是 W- 等价的，如果对于任意 $\alpha\in K$, 总有某个 $w\in W$ 以及某个 $a\in F$, 使得 $w(a-\alpha)\geqslant 0$. 特别地，当 $W=\{w\}$ 时，我们径称 F 和 K 是 w- 等价的.

引理 4.5.3 设 K 是域 F 的一个扩张， w 是域 K 的一个非浅显赋值， A 是 w 的赋值环. 如果 K 没有包含 A 的一阶赋值环，且对于 K 的任意非浅显赋值 v, 只要 v 的赋值环包含 A, v 的剩余域与 $v\mid_F$ 的剩余域相同，则 F 和 K 是 w- 等价的.

证明 假若引理不成立，则有某个 $\alpha\in K$, 使得对于每个 $a\in F$, 均有 $w(a-\alpha)<0$. 此时，显然 $\alpha\notin A$.

构造如下集合：

$$\Xi=\{B\mid B \text{ 是 } K \text{ 的赋值环，使得 } A\subseteq B, \text{ 但 } \alpha\notin B\}.$$

显然， $A\in\Xi$, 且 Ξ 对于集合的包含关系是一个偏序集.

设 $\{B_\lambda\mid\lambda\in\Lambda\}$ 是 Ξ 中任意一个链. 令 $B=\bigcup\limits_{\lambda\in\Lambda}B_\lambda$. 显然， B 是 K 的一个包含赋值环 A 的子环，从而 B 也是 K 的一个赋值环. 很清楚， $\alpha\notin B$. 因而 $B\in\Xi$, 即链 $\{B_\lambda\mid\lambda\in\Lambda\}$ 在 Ξ 中有一个上界 B. 由 Zorn 引理， Ξ 中有一个极大

元 C. 此时, 可断言 $K=C[\alpha]$. 事实上, 如若不然, 则 $C[\alpha]$ 是 K 的一个包含 A 的非浅显赋值环. 令 v_1 是由 $C[\alpha]$ 所确定的赋值. 由所设知, v_1 的剩余域与 $v_1|_F$ 的剩余域相同. 从而有 $a\in F$, 使得 $a-\alpha\in M_{v_1}$, 这里 M_{v_1} 是 v_1 的赋值理想. 注意到 $A\subseteq C[\alpha]$, 从而 $M_{v_1}\subseteq M_w$, 这里 M_w 为 w 的赋值理想. 于是 $a-\alpha\in M_w$, 即 $w(a-\alpha)>0$, 矛盾.

设 D 是域 K 的任意赋值环, 使得 $C\subseteq D$. 由 C 的极大性可知, $\alpha\in D$. 从而 $D\supseteq C[\alpha]=K$, 即 $D=K$. 这表明: C 是 K 的一阶赋值环; 矛盾于所设. 因此, F 和 K 是 w- 等价的. 证毕.

现在, 我们可以建立下面定理:

定理 4.5.4 设 (F,P) 是一个非阿基米德序域, 则下列叙述等价:

(1) (F,P) 具有弱 Hilbert 性质;

(2) 对于 F 的每个与 P 相容的非浅显赋值 v, v 的值群是可除的, 且其剩余域为实闭域;

(3) F 有一个与 P 相容的非浅显赋值 v, 满足下列条件: 对于 F 的每个非浅显的赋值 u, 只要 u 的赋值环 A_u 包含 v 的赋值环 A_v, u 的值群总是可除的, 且 u 的剩余域为实闭域;

(4) (F,P) 的实闭包 R 有一个非浅显的实赋值 w, 使得 F 和 R 是 w- 等价的.

证明 (1) $\Longrightarrow$ (2) 由命题 4.5.1 可知.

(2) $\Longrightarrow$ (3) 由命题 3.2.3 知, F 有一个非浅显的赋值 v 与 P 相容. 设 u 是 F 的一个非浅显赋值, 使得 $A_v\subseteq A_u$, 则 $M_u\subseteq M_v$, 这里 M_v 与 M_u 分别为 v 与 u 的赋值理想. 由于 v 与 P 相容, 从而由命题 3.1.3 知, $1+M_v\subseteq P$. 由此有, $1+M_u\subseteq 1+M_v\subseteq P$. 再由命题 3.1.3 知, u 与 P 相容. 由叙述 (2) 即知, u 的值群是可除的, 且其剩余域是实闭域.

(3) $\Longrightarrow$ (4) 设 v 是 F 的一个满足叙述 (3) 中条件的非浅显赋值. 由定理 3.2.5 知, v 可拓展为 R 的一个实赋值 w, 且 w 与 R 的惟一序 $\leqslant_{R^2}$ 相容. 对如下两种情况进行讨论:

情况 1 F 有一个一阶赋值 u, 使得 $A_v\subseteq A_u$. 此时, 由叙述 (3) 知, u 的值群是可除的, 且其剩余域是实闭域. 注意到, u 与 P 相容. 由命题 4.5.2 知, (F,P) 具有弱 Hilbert 性质. 根据定理 4.2.4, F 在 (F,P) 的实闭包 R 中稠密. 对于任意 $\alpha\in K$, 由 F 在 R 中的稠密性知, 有 $a\in F$, 使得 $|a-\alpha|_{R^2}<_{R^2}1$. 再由 w 和 $\leqslant_{R^2}$ 的相容性知, $w(a-\alpha)=w(|a-\alpha|_{R^2})\geqslant w(1)=0$. 这表明 F 和 R 是 w- 等价的.

情况 2 F 没有一阶赋值, 使得它的赋值环包含 A_v. 令 B_w 是赋值 w 的赋值环, 则 R 没有一阶赋值, 使它的赋值环包含 B_w. 设 w_1 是 R 的任意一个非浅显的赋值, 使得 $B_w\subseteq B_{w_1}$, 这里 B_{w_1} 为 w_1 的赋值环, 则 $w_1|_F$ 是 F 的一个非浅显赋值, 且它的赋值环为 $B_{w_1}\cap F$. 注意到 $A_v=B_w\cap F\subseteq B_{w_1}\cap F$. 从而由叙述 (3)

知，$w_1\mid_F$ 的剩余域是实闭域．于是 $w_1\mid_F$ 和 w_1 必定具有相同的剩余域．由引理 4.5.3 知，F 和 R 是 w- 等价的．

(4) $\Longrightarrow$ (1) 由定理 4.2.4 知，只需证明：F 在实闭包 R 中稠密．设 $\alpha\in R$，$e\in P$ 且 $e\neq 0$．由于 w 是 R 的非浅显赋值，从而 w 在 F 上的限制 $w\mid_F$ 是 F 的非浅显赋值．于是有 $c\in F$，使得 $w(c)>0$．由叙述 (4) 知，有 $a\in F$，使得 $w(e^{-1}c^{-1}\alpha-a)\geqslant 0$．由此有 $w(\alpha-aec)\geqslant w(ec)=w(e)+w(c)>w(e)$，即 $w(|\alpha-aec|_{R^2})>w(e)$．由于 w 与 $\leqslant_{R^2}$ 是相容的，从而必有 $|\alpha-aec|_{R^2}<_{R^2}e$，其中 $aec\in F$．因而，F 在 R 中稠密．证毕．

现设 (F,T) 是一个亚序域，K 是 (F,T) 的一个实扩张，则 K 的如下子集

$$S_K(T)=\left\{\sum_{i=1}^{n}t_i\alpha_i^2\mid n\text{为自然数},t_i\in T,\alpha_i\in K,i=1,\cdots,n\right\}$$

是 K 的一个亚正锥．依照 §3.2 中的讨论，对于任意 $Q\in\mathcal{X}_K(S_K(T))$，域 K 有一个关于序 $\leqslant_Q$ 的典型赋值 v_Q，使得 v_Q 的赋值环为典型赋值环 $A(\mathbb{Q},Q)$．用 $\mathcal{V}_K(T)$ 表示域 K 的所有这样的典型赋值 v_Q 所组成的集合，其中 $Q\in\mathcal{X}_K(S_K(T))$．

定理 4.5.5 设 (F,T) 是一个亚序域，则 (F,T) 具有弱 Hilbert 性质，当且仅当对于 (F,T) 的每个有限的实扩张 K，F 和 K 是 $\mathcal{V}_K(T)$- 等价的．

证明 必要性：设 (F,T) 具有弱 Hilbert 性质．由定理 4.4.5 知，(F,T) 是局部稠密的．对于任意 $\alpha\in K$，从而有 $a\in F$，使得对于某个 $Q\in\mathcal{X}(S_K(T))$，$|a-\alpha|_Q<_Q 1$．注意到，典型赋值 v_Q 与 Q 相容．从而，$v_Q(a-\alpha)=v_Q(|a-\alpha|_Q)\geqslant v_Q(1)=0$．由定义 4.5.1 知，$F$ 和 K 是 $\mathcal{V}_K(T)$- 等价的．

充分性：由定理 4.4.5 知，只需证明 (F,T) 是局部稠密的．设 K 是 (F,T) 的任意一个有限实扩张．对于任意 $\alpha\in K$ 以及非零 $e\in T$，由所设有 $a\in F$，使得 $v_Q(e^{-1}\alpha-a)\geqslant 0$，其中 $Q\in\mathcal{X}_K(S_K(T))$．于是 $e^{-1}\alpha-a\in A(\mathbb{Q},Q)$，即对于某个正有理数 q_1，$|e^{-1}\alpha-a|_Q<_Q q_1$．于是，集合 $\{q\in\mathbb{Q}\mid |e^{-1}\alpha-a|_Q<_Q q\}$ 是一个以 0 为下界的非空实数集．从而，该集合有下确界 $r\in\mathbb{R}$．显然，$r\geqslant 0$．取 $q\in\mathbb{Q}$，使得 $r<q<r+1$，即 $q-1<r<q$．由下确界的定义可得，$q-1<_Q|e^{-1}\alpha-a|_Q<_Q q$．由此有 $|e^{-1}\alpha-a-q|_Q<_Q 1$ 或 $|e^{-1}\alpha-a+q|_Q<_Q 1$，即有 $|\alpha-ae-qe|_Q<_Q e$ 或 $|\alpha-ae+qe|_Q<_Q e$，其中 $ae\pm qe\in F$．由定理 4.4.4 知，(F,T) 是局部稠密的．证毕．

此外，可建立下面的结果．

定理 4.5.6 设 (F,T) 是一个具有弱 Hilbert 性质的亚序域，v 是 F 的一个非浅显赋值，$\mathcal{X}_F^v$ 是 F 的所有与 v 相容的正锥组成的集合．若 $P\in\mathcal{X}_F^v$ 关于 Harrison 拓扑是 $\mathcal{X}_F^v$ 的一个内点，则 F 在它关于 P 的实闭包中稠密．

证明 设 R 是序域 (F,P) 的实闭包，则 $\Omega=R(\sqrt{-1})$ 是域 F 的代数闭包．由

定理 3.2.5 知, v 可拓展为 R 的一个实赋值 w.

由于 P 是 $\mathcal{X}_F^v$ 的一个内点, 从而序空间 $\mathcal{X}_F$ 有一个基本开集 $H(a_1,\cdots,a_n)$, 其中 $a_1,\cdots,a_n\in\dot{F}$, 使得 $P\in H(a_1,\cdots,a_n)\subseteq\mathcal{X}_F^v$. 设 $\alpha\in R$, 且 α 在 Ω 中的全部 F- 共轭元为: $\alpha_1,\cdots,\alpha_m$, 则 $\alpha_i=\xi_i+\eta_i\sqrt{-1}$, 其中 $\xi_i,\eta_i\in R$, $i=1,\cdots,m$. 令 $K=F(\sqrt{a_1},\cdots,\sqrt{a_n},\xi_1,\cdots,\xi_m,\eta_1,\cdots,\eta_m)$, 则 K 是亚序域 (F,T) 的一个有限实扩张. 由于 (F,T) 具有弱 Hilbert 性质, 从而由定理 4.4.5 和定理 4.4.4 可知, K 有一个包含 T 的正锥 Q, 且 F 中有元素 $b_1,\cdots,b_m,c_1,\cdots,c_m$, 使得 $|\xi_i-b_i|_Q<_Q 1$, 且 $|\eta_i-c_i|_Q<_Q 1$, $i=1,\cdots,m$. 令 $P_1=Q\cap F$, 则 $a_i=(\sqrt{a_i})^2\in Q\cap F=P_1$, $i=1,\cdots,n$. 这表明: $P_1\in H(a_1,\cdots,a_n)\subseteq\mathcal{X}_F^v$, 即 v 与 P_1 相容. 设 R_1 是序域 (K,Q) 在 Ω 中的实闭包, 则 R_1 实际上也是序域 (F,P_1) 的实闭包. 由定理 3.2.5 知, v 可拓展为 R_1 的一个实赋值 w_1.

根据命题 3.4.3, w 和 w_1 都是 Hensel 赋值, 从而它们在 Ω 上的拓展都是惟一的. 为节省符号, w 和 w_1 在 Ω 上的惟一拓展仍分别记作 w 和 w_1. 此时, 显然有下列事实:

$$\text{对于任意 } x,\ y\in R,\ w(x+y\sqrt{-1})=w(x-y\sqrt{-1}).$$

由于 w 与 w_1 都是赋值 v 在 Ω 上的拓展, 从而由赋值论知, 存在域 Ω 的一个 F-自同构 π, 使得对于每个 $z\in\Omega$, $w(z)=w_1(\pi(z))$. 此时, 对于某个 $k\in\{1,\cdots,m\}$, $\pi(\alpha)=\alpha_k$.

注意到, w_1 与 R_1 的惟一正锥 R_1^2 相容. 从而有 $w_1(\xi_i-b_i)=w_1(|\xi_i-b_i|_Q)\geqslant w_1(1)=0$, 且 $w_1(\eta_i-c_i)=w_1(|\eta_i-c_i|_Q)\geqslant w_1(1)=0$, $i=1,\cdots,m$. 显然 $w_1(\sqrt{-1})=\frac{1}{2}w_1(-1)=0$. 由此有

$$\begin{aligned}w_1(\alpha_k-b_k-c_k\sqrt{-1})=w_1((\xi_k-b_k)+(\eta_k-c_k)\sqrt{-1})\geqslant\\ \min\{w_1(\xi_k-b_k),w_1(\eta_k-c_k)\}\geqslant 0.\end{aligned}$$

当 $\pi(\sqrt{-1})=\sqrt{-1}$ 时, 上式为 $w_1(\pi(\alpha-b_k-c_k\sqrt{-1}))\geqslant 0$, 即有 $w(\alpha-b_k-c_k\sqrt{-1})\geqslant 0$. 由上面事实又有 $w(\alpha-b_k+c_k\sqrt{-1})\geqslant 0$. 当 $\pi(\sqrt{-1})=-\sqrt{-1}$ 时, 上式为 $w_1(\pi(\alpha-b_k+c_k\sqrt{-1}))\geqslant 0$, 即有 $w(\alpha-b_k+c_k\sqrt{-1})\geqslant 0$. 同样, 又有 $w(\alpha-b_k-c_k\sqrt{-1})\geqslant 0$. 于是总有 $2w(\alpha-b_k)=w((\alpha-b_k)^2)\geqslant w((\alpha-b_k)^2+c_k^2)=w(\alpha-b_k+c_k\sqrt{-1})+w(\alpha-b_k-c_k\sqrt{-1})\geqslant 0$. 从而 $w(\alpha-b_k)\geqslant 0$, 其中 $b_k\in F$. 这表明: F 和 R 是 w- 等价的. 由定理 4.5.4 知, 序域 (F,P) 具有弱 Hilbert 性质. 再由定理 4.2.4 知, F 在实闭包 R 中稠密. 证毕.

上面定理可看做定理 4.4.6 的一个改进. 事实上, 当定理 4.4.6 的所设条件都成立时, 令 v 是 F 的关于序 P 的典型实赋值. 若 P 是 F 的阿基米德正锥, 则 F 显然在 (F,P) 的实闭包中稠密. 若 P 不是 F 的阿基米德正锥, 则 v 是 F 的非浅

显赋值. 由定理 4.4.6 中所设, P 是 $\mathcal{X}_F^v$ 的一个内点. 从而由上面的定理 4.5.6 即知, P 在 (F,P) 的实闭包中稠密.

由上面的定理 4.5.6, 我们还可以建立下面结论.

定理 4.5.7 设 (F,T) 是一个仅有有限个阿基米德序的亚序域, 且 F 有有限个非浅显的赋值 $v_1,\cdots,v_m$, 使得 $\mathcal{X}_F^{v_1}\cup\cdots\cup\mathcal{X}_F^{v_m}$ 恰好由 F 的全部非阿基米德正锥组成, 则 (F,T) 具有弱 Hilbert 性质, 当且仅当 F 在 (F,T) 的每个实闭包中稠密.

证明 充分性显然, 只须证明必要性. 显然, 可进一步假定: 对于任意相异的 $i,j\in\{1,\cdots,m\}$, $\mathcal{X}_F^{v_i}\not\subseteq\mathcal{X}_F^{v_j}$; 否则去掉赋值 v_i 后, 定理的条件仍成立. 令 A_i 为 v_i 的赋值环, $i=1,\cdots,m$. 此时可断言: 对于相异的 $i,j\in\{1,\cdots,m\}$, $A_i\not\subseteq A_j$. 事实上, 如若 $A_i\subseteq A_j$, 则 $M_j\subseteq M_i$, 其中 M_i 和 M_j 分别为 A_i 和 A_j 的赋值理想. 对于每个 $P\in\mathcal{X}_F^{v_i}$, 由命题 3.1.3 知, $1+M_j\subseteq 1+M_i\subseteq P$. 从而又有 $P\in\mathcal{X}_F^{v_j}$, 即 $\mathcal{X}_F^{v_i}\subseteq\mathcal{X}_F^{v_j}$; 矛盾于我们的假定.

设 $P\in\mathcal{X}_F$. 当 P 是阿基米德正锥时, F 显然在它关于 P 的实闭包中稠密. 当 P 是非阿基米德正锥时, 由所设知, $P\in\mathcal{X}_F^{v_1}\cup\cdots\cup\mathcal{X}_F^{v_m}$. 不失一般性, 不妨设 $P\in\mathcal{X}_F^{v_1}$. 根据定理 4.5.6, 为证明 F 在它关于 P 的实闭包中稠密, 只须证明: $\mathcal{X}_F^{v_1}$ 对于 Harrison 拓扑是一个开子集. 由于 v_1 是 F 的非浅显赋值, 从而 $A_1\neq F$, 即有 $a\in F$, 使得 $a\notin A_1$. 此时, 显然 $a^2\notin A_1$.

设 $P_1,\cdots,P_r$ 是 (F,T) 的全部阿基米德正锥, 则对于每个 $j=1,\cdots,r$, 有正有理数 q_j, 使得 $a^2<_{P_j}q_j$. 令 $q=\max\{q_j\mid j=1,\cdots,r\}$, 则 $a^2<_{P_j}q$ 即 $q-a^2\in P_j$, $j=1,\cdots,r$.

由于 $A_1\not\subseteq A_i$, 且 $A_i\not\subseteq A_1$, $i=2,\cdots,m$. 从而有 $d_i\in A_1$, 使得 $d_i\notin A_i$, 且有 $e_i\in A_i$, 使得 $e_i\notin A_1$, $i=2,\cdots,m$.

下面证明: $\mathcal{X}_F^{v_1}=H(a^2-q,e_2^2-d_2^2,\cdots,e_m^2-d_m^2)$. 事实上, 设 $P\in\mathcal{X}_F^{v_1}$. 假若 $a^2-q\notin P$, 则有 $0<_P a^2<_P q\in A_1$. 由 v_1 和 P 的相容性有 $a^2\in A_1$, 得出矛盾. 从而 $a^2-q\in P$. 又假若 $e_k^2-d_k^2\notin P$, $2\leqslant k\leqslant m$, 则有 $0<_P e_k^2<_P d_k^2\in A_1$. 由此可得 $e_k^2\in A_1$, 即 $e_k\in A_1$, 又得出矛盾. 因而, $e_i^2-d_i^2\in P$, $i=2,\cdots,m$. 因此 $P\in H(a^2-q,e_2^2-d_2^2,\cdots,e_m^2-d_m^2)$. 反过来, 设 $P\in H(a^2-q,e_2^2-d_2^2,\cdots,e_m^2-d_m^2)$, 则 $q-a^2\notin P$. 由 q 的选取可知, P 不是 (F,T) 的阿基米德正锥. 假若 $P\in\mathcal{X}_F^{v_k}$, $2\leqslant k\leqslant m$, 则由关系式 $0<_P d_k^2<_P e_k^2\in A_k$, 可推得 $d_k\in A_k$, 矛盾于 d_k 的选取. 从而 $P\notin\mathcal{X}_F^{v_2}\cup\cdots\cup\mathcal{X}_F^{v_m}$. 由此必有 $P\in\mathcal{X}_F^{v_1}$. 于是, $\mathcal{X}_F^{v_1}=H(a^2-q,e_1^2-d_1^2,\cdots,e_m^2-d_m^2)$. 因此, $\mathcal{X}_F^{v_1}$ 是一个开子集. 证毕.

有例子表明, 在上面定理中, 条件 "仅有有限个阿基米德正锥" 不是多余的. 有兴趣的读者可参见文献 [215].

§4.6 强局部稠密性与弱 Hilbert 性质的升降

在 §4.4 中，我们引进了亚序域的 "局部稠密性" 这一概念，从而刻画了具有弱 Hilbert 性质的亚序域. 在本节中，我们将进一步在亚序域范畴中引进 "强局部稠密性" 这一概念，同时证明 "强局部稠密性", "局部稠密性" 与 "弱 Hilbert 性质" 之间的等价性. 此外，我们还研究弱 Hilbert 性质对于亚序域的有限生成扩张的上升性与下降性.

设 (F,T) 是一个亚序域. 一个域 K 称做 (F,T) 的一个有限生成实扩张，如果 K 是域 F 的一个有限生成扩张，且 K 是亚序域 (F,T) 的实扩张. 显然，亚序域 (F,T) 的有限实扩张必为有限生成实扩张.

定义 4.6.1 一个亚序域 (F,T) 称做是强局部稠密的，如果对于 (F,T) 的每个有限生成实扩张 K 以及任意两个相异的 $\alpha,\beta\in K$, K 有一个包含 T 的正锥 Q, 且有 $a\in F$, 使得 $a\in]\alpha,\beta[_Q$, 这里 $]\alpha,\beta[_Q$ 的意义同定义 4.4.1.

显然，若亚序域 (F,T) 是强局部稠密的，则 (F,T) 是局部稠密的. 下面证明：对于亚序域来说，强局部稠密性实际上等价于局部稠密性，自然也等价于弱 Hilbert 性质.

定理 4.6.1 一个亚序域 (F,T) 具有弱 Hilbert 性质，当且仅当 (F,T) 是强局部稠密的.

证明 充分性：设 (F,T) 是强局部稠密的，则 (F,T) 是局部稠密的. 由定理 4.4.5 知，(F,T) 具有弱 Hilbert 性质.

必要性：设 K 是 (F,T) 的任意一个有限生成的实扩张，$\alpha,\beta\in K$, 且 $\alpha\neq\beta$. 由于 K 在 F 上是有限生成的，从而有 $K=F(t_1,\cdots,t_m,\theta)$, 其中 $t_1,\cdots,t_m$ 是 K 在 F 上的一个超越基，θ 是域 $F(t_1,\cdots,t_m)$ 上一个代数元. 此时，$\alpha=\phi(t_1,\cdots,t_m,\theta)$, 而 $\beta=\psi(t_1,\cdots,t_m,\theta)$, 其中 $\phi(x_1,\cdots,x_m,x_{m+1})$ 和 $\psi(x_1,\cdots,x_m,x_{m+1})$ 都是域 F 上含未定元 $x_1,\cdots,x_m,x_{m+1}$ 的有理函数. 取 $g\in F[x_1,\cdots,x_m,x_{m+1}]$, 使得 $g\phi$, $g\psi\in F[x_1,\cdots,x_m,x_{m+1}]$, 且 $g(t_1,\cdots,t_m,\theta)\neq 0$.

设 θ 在 $F(t_1,\cdots,t_m)$ 上的极小多项式为

$$G(\bar{t};y)=y^d+e_1(\bar{t})y^{d-1}+\cdots+e_d(\bar{t}),$$

其中 $e_i(\bar{t})\in F(t_1,\cdots,t_m)$, $i=1,\cdots,d$.

由于 K 是 (F,T) 的实扩张，从而 K 有一个正锥 Q_K, 使得 $T\subseteq Q_K$. 于是，多项式 $G(\bar{t};y)$ 在序域 $(F(t_1,\cdots,t_m),Q_K\cap F(t_1,\cdots,t_m))$ 的序代数扩张 (K,Q_K) 中有一个根 θ.

令 $G_0(\bar{t};y)$, $G_1(\bar{t};y)$, $\cdots$, $G_k(\bar{t};y)$ 是多项式 $G(\bar{t};y)$ 和它关于变量 y 的微商 $G'_y(\bar{t};y)$ 的 Sturm 序列，其中 $G_i(\bar{t};y)\in F(t_1,\cdots,t_m)[y]$, $i=0,1,\cdots,k$. 而且，

用 $\{c_j(\bar{t}) \mid j=1, \cdots, r\}$ 表示诸多项式 $G_0(\bar{t};y)$, $G_1(\bar{t};y)$, $\cdots$, $G_k(\bar{t};y)$ 的所有非零系数. 显然, $c_j(\bar{t}) \in F(t_1,\cdots,t_m)$, $j=1,\cdots,r$. 从而有 $h(\bar{t}) \in F[t_1,\cdots,t_m]$, 使得 $h(\bar{t})c_j(\bar{t}) \in F[t_1,\cdots,t_m]$, $j=1,\cdots,r$. 显然 α, β, $c_j(\bar{t}) \in F[t_1,\cdots,t_m,\theta,g^{-1}(t_1,\cdots,t_m,\theta),h^{-1}(\bar{t})]$, $j=1,\cdots,r$.

由定理 3.6.7 知, 有一个从 $F[t_1,\cdots,t_m,\theta,\alpha,\beta,h^{-1}(\bar{t})]$ 到序域 $(F,Q_K\cap F)$ 的实闭包 R 的一个 F- 代数同态 σ, 使得

(1) $\sigma(\alpha)\neq\sigma(\beta)$, 即

$$\phi(\sigma(t_1),\cdots,\sigma(t_m),\sigma(\theta))\neq\psi(\sigma(t_1),\cdots,\sigma(t_m),\sigma(\theta));$$

(2) $c_j(\sigma(t_1),\cdots,\sigma(t_m))\neq 0$, $j=1,\cdots,r$;

(3) $g(\sigma(t_1),\cdots,\sigma(t_m),\sigma(\theta))\neq 0$.

令 $K_1=F(\sigma(t_1),\cdots,\sigma(t_m),\sigma(\alpha),\sigma(\beta),\sigma(\theta))$, 则 $K_1\subseteq R$. 从而 K_1 是 (F,T) 的一个有限实扩张. 由定理 4.4.5 知, (F,T) 是局部稠密的. 从而 K_1 有一个包含 T 的正锥 Q_1, 且有 $a\in F$, 使得 $a\in]\sigma(\alpha),\sigma(\beta)[_{Q_1}$.

设 R_1 是序域 (K_1,Q_1) 的实闭包, 且记 $e_i(\overline{\sigma(t)})=e_i(\sigma(t_1),\cdots,\sigma(t_m))$, $i=1$, $\cdots$, d, 而 $G_j(\overline{\sigma(t)};y)=G_j(\sigma(t_1),\cdots,\sigma(t_m);y)$, $j=0$, 1, $\cdots$, k. 此时, 多项式 $G(\overline{\sigma(t)};y)=y^d+e_1(\overline{\sigma(t)})y^{d-1}+\cdots+e_d(\overline{\sigma(t)})$ 在 R_1 中有根 $\sigma(\theta)$, 且 $G_0(\overline{\sigma(t)};y)$, $G_1(\overline{\sigma(t)};y)$, $\cdots$, $G_k(\overline{\sigma(t)};y)$ 是 R_1 上多项式 $G(\overline{\sigma(t)};y)$ 与它的微商的 Sturm 序列. 选取足够小的 $\delta\in R_1^2$, 使得诸多项式 $G_j(\overline{\sigma(t)};y)$ 在闭区间 $[\sigma(\theta)-\delta,\sigma(\theta)+\delta]_{R_1^2}$ 中除 $\sigma(\theta)$ 外没有其他根, $j=0$, 1, $\cdots$, k. 由 Sturm 定理 (定理 2.4.6) 知, 变号数差

$$\begin{aligned}&v\big(G_0(\overline{\sigma(t)};y),G_1(\overline{\sigma(t)};y);\sigma(\theta)-\delta\big)\\ -\ &v\big(G_0(\overline{\sigma(t)};y),G_1(\overline{\sigma(t)};y);\sigma(\theta)+\delta\big)=1.\end{aligned}$$

设 $\eta_1,\cdots,\eta_m$ 是域 R_1 上 m 个未定元. 由定理 2.6.3 知, 域 $L=R_1(\eta_1,\cdots,\eta_m)$ 有一个正锥 P_L, 使得 η_1, $\cdots$, η_m 在 R_1 上都是无限小元素. 记 R_L 为序域 (L,P_L) 的实闭包. 由元素 η_1, $\cdots$, η_m 在 R_1 上的无限小性可知, $G_j(\overline{\sigma(t)+\eta};\sigma(\theta)\pm\delta):=G_j(\sigma(t_1)+\eta_1,\cdots,\sigma(t_m)+\eta_m;\sigma(\theta)\pm\delta)$ 关于正锥 R_L^2 的符号相同于 $G_j(\overline{\sigma(t)};\sigma(\theta)\pm\delta)$ 关于 R_1^2 的符号. 从而, 变号数差

$$\begin{aligned}&v\big(G_0(\overline{\sigma(t)+\eta};y),G_1(\overline{\sigma(t)+\eta};y);\sigma(\theta)-\delta\big)\\ -\ &v\big(G_0(\overline{\sigma(t)+\eta};y),G_1(\overline{\sigma(t)+\eta};y);\sigma(\theta)+\delta\big)=1.\end{aligned}$$

显然, $G_0(\overline{\sigma(t)+\eta};y)$, $G_1(\overline{\sigma(t)+\eta};y)$, $\cdots$, $G_k(\overline{\sigma(t)+\eta};y)$ 恰好是 R_L 上多项式 $G(\overline{\sigma(t)+\eta};y)$ 和它的微商的 Sturm 序列. 由 Sturm 定理可知, 多项式 $G(\overline{\sigma(t)+\eta};y)$ 在开区间 $]\sigma(\theta)-\delta,\sigma(\theta)+\delta[_{R_L^2}$ 中恰有一个根 θ_1. 由于 δ 可以选取 R_1^2 中任意尽可能小的元素, 从而 $\theta_1-\sigma(\theta)$ 关于正锥 R_L^2 是在 R_1 上的无限小元素.

由于 $\eta_1, \cdots, \eta_m, \theta_1 - \sigma(\theta)$ 关于 R_L^2 是 R_1 上的无限小元素，且 a 介于两元素 $\sigma(\alpha) = \phi(\sigma(t_1), \cdots, \sigma(t_m), \sigma(\theta))$ 和 $\sigma(\beta) = \psi(\sigma(t_1), \cdots, \sigma(t_m), \sigma(\theta))$ 之间，从而 a 介于 $\phi(\sigma(t_1) + \eta_1, \cdots, \sigma(t_m) + \eta_m, \theta_1)$ 和 $\psi(\sigma(t_1) + \eta_1, \cdots, \sigma(t_m), \theta_1)$ 之间，即有

$$a \in]\phi(\overline{\sigma(t) + \eta}, \theta_1), \psi(\overline{\sigma(t) + \eta}, \theta_1)[_{R_L^2}.$$

显然，有一个 K 到 R_L 的一个 F- 嵌入 π, 使得 $\pi(t_i) = \sigma(t_i) + \eta_i$, $i = 1, \cdots, m$, 且 $\pi(\theta) = \theta_1$. 令 $Q = \pi^{-1}(R_L^2)$, 则 Q 显然是 K 的一个包含 T 的正锥. 由于 $\pi(a) = a \in]\phi(\overline{\sigma(t) + \eta}, \theta_1), \psi(\overline{\sigma(t) + \eta}, \theta_1)[_{R_L^2} =]\pi(\alpha), \pi(\beta)[_{R_L^2}$, 从而 $a \in]\alpha, \beta[_Q$. 因此，(K, T) 是强局部稠密的. 证毕.

此外，亚序域的弱 Hilbert 性质还可以通过实函数域的实位来刻画. 在此之前，我们需要下面有用的引理:

引理 4.6.2 设亚序域 (F,T) 是强局部稠密的，则对于 (F,T) 的每个有限生成的实扩张 K 以及 K 中任意有限个元素 $\alpha_1, \cdots, \alpha_m$ 和 $\beta_1, \cdots, \beta_m$, 其中 $\alpha_i \neq \beta_i$, $i = 1, \cdots, m$, 总有 $a_1, \cdots, a_m \in F$, 使得 $a_i \in]\alpha_i, \beta_i[_Q$, $i = 1, \cdots, m$, 这里 Q 是 K 的某个包含 T 的正锥.

证明 对 m 施用归纳法. 当 $m = 1$ 时，由定义 4.6.1 知，引理成立. 假定在 $m = k$ 时引理成立，现考虑 $m = k + 1$ 的情形. 由归纳假定，K 有一个包含 T 的正锥 Q_1, 且有 $a_1, \cdots, a_k \in F$, 使得 $a_i \in]\alpha_i, \beta_i[_{Q_1}$, $i = 1, \cdots, k$. 此时有，$(\frac{\alpha_i + \beta_i}{2} - a_i)^2 - (\frac{\alpha_i - \beta_i}{2})^2 \in Q_1$, $i = 1, \cdots, k$. 令 R 是序域 (K, Q_1) 的实闭包，且令 $L = K\left(\sqrt{(\frac{\alpha_1+\beta_1}{2} - a_1)^2 - (\frac{\alpha_1-\beta_1}{2})^2}, \cdots, \sqrt{(\frac{\alpha_k+\beta_k}{2} - a_k)^2 - (\frac{\alpha_k-\beta_k}{2})^2}\right) \subseteq R$, 则 L 也是 (F,T) 的一个有限生成的实扩张. 由于 (F,T) 是强局部稠密的，从而 L 有一个包含 T 的正锥 Q_L, 且有 $a_{k+1} \in F$, 使得 $a_{k+1} \in]\alpha_{k+1}, \beta_{k+1}[_{Q_L}$. 令 $Q = Q_L \cap K$, 则显然 Q 是 K 的一个包含 T 的正锥. 此时易见，$a_i \in]\alpha_i, \beta_i[_Q$, $i = 1, \cdots, k+1$. 从而，引理在 $m = k + 1$ 时成立. 由归纳法原理，引理获证.

现在，我们来证明如下定理.

定理 4.6.3 设 (F,T) 是一个亚序域，则下列叙述等价:

(1) (F,T) 具有弱 Hilbert 性质;

(2) 若 K 是 (F,T) 的一个有限生成实扩张，$t_1, \cdots, t_m$ 是 K 在 F 上的一个超越基，$\xi \in K$ 但 $\xi \notin S_K(T)$, 则 K 有一个代数的 F- 位 ϕ, 且 $\phi(K)$ 有一个包含 T 的正锥 P, 使得 $\phi(t_i) \in F$, $i = 1, \cdots, m$, 且 $\phi(\xi) <_P 0$.

证明 (2) $\Longrightarrow$ (1): 由定理 4.4.5 的推论 1 知，只须证明：(F,T) 上每个单元半正定多项式同时也是强半正定的. 设 $f(x) \in F[x]$, 且 $f(x)$ 在 (F,T) 上是半正定的. 假若 $f(x)$ 在 (F,T) 上不是强半正定的，则由定理 4.1.3 知，$f(x) \notin S_{F(x)}(T)$. 注意到 $F(x)$ 是 (F,T) 的一个有限生成实扩张，且 x 是 $F(x)$ 在 F 上的一个超越基.

由叙述 (2) 知, $F(x)$ 有一个代数的 F- 位 ϕ, 且 $\phi(F(x))$ 有一个包含 T 的正锥 P, 使得 $\phi(x)=a\in F$, 且 $\phi(f(x))<_P 0$. 此时, 显然 $\phi(F(x))=F$, 且 $\phi(f(x))=f(a)$. 从而 P 实际上是 (F,T) 的一个正锥, 使得 $f(a)<_P 0$, 矛盾于 $f(x)$ 在 (F,T) 上的半正定性. 因此, $f(x)$ 在 (F,T) 上是强半正定的. 叙述 (1) 获证.

(1) $\Longrightarrow$ (2): 由所设知, $S_K(T)$ 是 K 的一个亚正锥. 由定理 1.1.2 知, K 有一个正锥 Q_1, 使得 $\xi\notin Q_1$, 即 $\xi<_{Q_1}0$.

设 $K=F(t_1,\cdots,t_m,\alpha)$, 其中 α 是域 $F(t_1,\cdots,t_m)$ 上代数元. 不妨设 α 在 $F(t_1,\cdots,t_m)$ 上的极小多项式为

$$f(t_1,\cdots,t_m;x)=x^d+c_1(\bar{t})x^{d-1}+\cdots+c_d(\bar{t}),$$

其中 $c_i(\bar{t})\in F[t_1,\cdots,t_m]$, $i=1,\cdots,d$.

由于 $\xi\in K$, 从而 ξ 可表示如下:

$$\xi=g(t_1,\cdots,t_m;\alpha)h(t_1,\cdots,t_m;\alpha)^{-1},$$

其中 $g(t_1,\cdots,t_m;x)$, $h(t_1,\cdots,t_m;x)\in F[t_1,\cdots,t_m,x]$.

令 $e(t_1,\cdots,t_m;x)=g(t_1,\cdots,t_m;x)h(t_1,\cdots,t_m;x)\in F[t_1,\cdots,t_m,x]$, 则有

$$\xi=e(t_1,\cdots,t_m;\alpha)h(t_1,\cdots,t_m;\alpha)^{-2}, \text{且 } e(t_1,\cdots,t_m;\alpha)<_{Q_1}0.$$

令 R_1 是序域 (K,Q_1) 的实闭包, 则 $f(t_1,\cdots,t_m;x)$ 在 R_1 中不可能有重根. 从而有 $\delta\in S_F$, 使得 $f(t_1,\cdots,t_m;x)$ 在开区间 $]\alpha-\delta,\alpha+\delta[_{R_1^2}$ 内只有惟一单根. 由引理 4.4.3 知, 有非零 $d\in S_K$, 使得对于 K 的每个实闭包 R 以及 R 中任意元素 $z_1,\cdots,z_m$, y, 只要 $|z_i-t_i|_{R^2}<d$, $i=1,\cdots,m$, 且 $|y-\alpha|_{R^2}<d$, 总有 $e(t_1,\cdots,t_m;\alpha)e(z_1,\cdots,z_m;y)>_{R^2}0$. 注意到 $\dfrac{\delta d^2}{1+d^2}<_{R_1^2}\delta$, 从而 $f(t_1,\cdots,t_m;\alpha-\dfrac{\delta d^2}{1+d^2})f(t_1,\cdots,t_m;\alpha+\dfrac{\delta d^2}{1+d^2})<_{R_1^2}0$. 再由引理 4.4.3 知, 有非零 $d_1\in S_K$, 使得对于 K 的每个实闭包 R, 只要 $z_i\in R$ 且 $|z_i-t_i|_{R^2}<d_1$, $i=1,\cdots,m$, 总有

$$\begin{aligned}&f(t_1,\cdots,t_m;\alpha-\frac{\delta d^2}{1+d^2})f(t_1,\cdots,t_m;\alpha+\frac{\delta d^2}{1+d^2})\\ \cdot\ &f(z_1,\cdots,z_m;\alpha-\frac{\delta d^2}{1+d^2})f(z_1,\cdots,z_m;\alpha+\frac{\delta d^2}{1+d^2})>_{R^2}0.\end{aligned}$$

记 $\beta:=-f(t_1,\cdots,t_m;\alpha-\dfrac{\delta d^2}{1+d^2})f(t_1,\cdots,t_m;\alpha+\dfrac{\delta d^2}{1+d^2})$, 且考虑域 K 的如下扩张:

$$L=K(\sqrt{-e(t_1,\cdots,t_m;\alpha)},\sqrt{\beta}).$$

注意到 $L \subseteq R_1$, 从而 L 是 (F,T) 的有限实扩张. 由定理 4.6.1 知, (F,T) 是强局部稠密的. 由引理 4.6.2 知, L 有一个包含 T 的正锥 Q_L, 且有 $a_1, \cdots, a_m$, $b \in F$, 使得 $|a_i - t_i|_{Q_L} <_{Q_L} \dfrac{d^2 d_1^2}{(1+d^2)(1+d_1^2)}$, $i = 1, \cdots, m$, 且 $0 <_{Q_L} b <_{Q_L} (\sqrt{-e(t_1, \cdots, t_m; \alpha)})^2 = -e(t_1, \cdots, t_m; \alpha)$. 设 R_L 是序域 (L, Q_L) 的实闭包, 则 R_L 也是 K 的一个实闭包. 显然 $|a_i - t_i|_{Q_L} <_{Q_L} d_1$, $i = 1, \cdots, m$. 从而有

$$
\begin{aligned}
&f(t_1, \cdots, t_m; \alpha - \frac{\delta d^2}{1+d^2}) f(t_1, \cdots, t_m; \alpha + \frac{\delta d^2}{1+d^2}) \\
\cdot\ &f(a_1, \cdots, a_m; \alpha - \frac{\delta d^2}{1+d^2}) f(a_1, \cdots, a_m; \alpha + \frac{\delta d^2}{1+d^2}) >_{R_L^2} 0.
\end{aligned}
$$

注意到 $-f(t_1, \cdots, t_m; \alpha - \dfrac{\delta d^2}{1+d^2}) f(t_1, \cdots, t_m; \alpha + \dfrac{\delta d^2}{1+d^2}) = \beta^2 \in Q_L$, 于是有

$$
f(t_1, \cdots, t_m; \alpha - \frac{\delta d^2}{1+d^2}) f(t_1, \cdots, t_m; \alpha + \frac{\delta d^2}{1+d^2}) <_{R_L^2} 0.
$$

因而有

$$
f(a_1, \cdots, a_m; \alpha - \frac{\delta d^2}{1+d^2}) f(a_1, \cdots, a_m; \alpha + \frac{\delta d^2}{1+d^2}) <_{R_L^2} 0.
$$

设 $\eta_1, \cdots, \eta_m$ 是域 R_L 上 m 个未定元, 则 $E := R_L(\eta_1, \cdots, \eta_m)$ 有一个正锥 Q_E, 使得 $\eta_1, \cdots, \eta_m$ 在 R_L 上都是无限小元素. 令 R_E 为序域 (E, Q_E) 的实闭包. 由 $\eta_1, \cdots, \eta_m$ 的无限小性知, $f(a_1+\eta_1, \cdots, a_m+\eta_m; \alpha - \dfrac{\delta d^2}{1+d^2}) f(a_1+\eta_1, \cdots, a_m+\eta_m; \alpha + \dfrac{\delta d^2}{1+d^2}) <_{R_E^2} 0$. 由中间值定理, 有 $\alpha_1 \in R_E$, 使得 $f(a_1+\eta_1, \cdots, a_m+\eta_m; \alpha_1) = 0$, 且 $\alpha - \dfrac{\delta d^2}{1+d^2} <_{R_E^2} \alpha_1 <_{R_E^2} \alpha + \dfrac{\delta d^2}{1+d^2}$. 此时有 $|\alpha_1 - \alpha| <_{R_E^2} \dfrac{\delta d^2}{1+d^2} <_{R_E^2} d$, 且 $|a_i + \eta_i - t_i| <_{R_E^2} d$, $i = 1, \cdots, m$. 由 d 的选取知, $e(t_1, \cdots, t_m; \alpha) e(a_1 + \eta_1, \cdots, a_m + \eta_m; \alpha_1) >_{R_E^2} 0$. 注意到, $-e(t_1, \cdots, t_m; \alpha) - b \in Q_L \subseteq R_E^2$. 从而有 $e(a_1+\eta_1, \cdots, a_m+\eta_m; \alpha_1) + b <_{R_E^2} 0$, 即 $g(a_1+\eta_1, \cdots, a_m+\eta_m; \alpha_1) h^{-1}(a_1 + \eta_1, \cdots, a_m + \eta_m; \alpha_1) <_{R_E^2} 0$.

设 $D = F(\eta_1, \cdots, \eta_m, \alpha_1)$, 且 $Q_D = R_E^2 \cap D$, 则 $T \subseteq Q_D$, 且存在 K 到 D 的一个 F- 同构 π, 使得 $\pi(t_i) = a_i + \eta_i$, $i = 1, \cdots, m$, 且 $\pi(\alpha) = \alpha_1$. 令 R 是域 F 在 R_E 中的代数闭包, 显然 $T \subseteq R^2$. 根据定理 3.6.9 的证明可知, D 有一个与 Q_D 相容的代数的 F- 位 ψ: $D \longrightarrow R \cup \{\infty\}$, 使得 $\psi(\eta_i) = 0$, $i = 1, \cdots, m$. 注意到, 多项式 $f(a_1+\eta_1, \cdots, a_m+\eta_m; x)$ 是 $A_\psi[x]$ 中首项系数为 1 的多项式, 这里 A_ψ 为位 ψ 的赋值环. 从而 α_1 在 A_ψ 上整, 即有 $\alpha_1 \in A_\psi$. 由 ψ 和 Q_D 的相容性知, $\psi(e(a_1+\eta_1, \cdots, a_m+\eta_m; \alpha_1)+b) \leqslant_{R^2} 0$, 即有 $e(a_1, \cdots, a_m; \psi(\alpha_1)) <_{R^2} -b <_{R^2} 0$. 令

$\phi=\psi\circ\pi$, 则 ϕ 是 K 到 $R\cup\{\infty\}$ 的一个代数 F- 位. 此时, $\phi(e(t_1,\cdots,t_m;\alpha))<_{R^2}0$, 即有 $\phi(\xi)<_{R^2}0$. 因而, 叙述 (2) 获证. 证毕.

现在, 我们来研究弱 Hilbert 性质对于亚序域的有限生成扩张的上升性与下降性, 即考虑这样一个问题: 若亚序域 (K,S) 是亚序域 (F,T) 的一个有限生成扩张, 且其中一个亚序域具有弱 Hilbert 性质, 是否另一个亚序域也具有弱 Hilbert 性质?

定义 4.6.2 设 (F,T) 和 (K,S) 都是亚序域. (K,S) 称作 (F,T) 的一个有限生成扩张, 如果 K 是域 F 的一个有限生成扩张, 且存在有限个元素 $\alpha_1,\cdots,\alpha_m\in K$, 使得

$$S=\left\{\sum_{i=1}^{n}\alpha_1^{k_{i1}}\cdots\alpha_m^{k_{im}}t_i\beta_i^2 \mid n\text{为自然数}, t_i\in T, \beta_i\in K, k_{ij}=0\text{或}1, i=1,\cdots,n; j=1,\cdots,m\right\}.$$

下面的定理表明: 弱 Hilbert 性质对于亚序域的有限生成扩张的上升性是成立的.

定理 4.6.4 设 (F,T) 和 (K,S) 均为亚序域, 且 (K,S) 是 (F,T) 的有限生成扩张. 若 (F,T) 具有弱 Hilbert 性质, 则 (K,S) 也具有弱 Hilbert 性质.

证明 由定理 4.6.1 知, 只须证明: (K,S) 是强局部稠密的. 由条件, 可设 S 为定义 4.6.2 中所示的集合. 设 L 是 (K,S) 的任意一个有限生成实扩张, $\alpha,\beta\in L$, 且 $\alpha\neq\beta$. 由于 L 是 (K,S) 的一个实扩张, 从而 L 有一个正锥 Q_1, 使得 $S\subseteq Q_1$. 令 R_1 是序域 (L,Q_1) 的实闭包, 且 $E=L(\sqrt{\alpha_1},\cdots,\sqrt{\alpha_m})$, 则 $E\subseteq R_1$, 且 $\alpha,\beta\in E$. 于是, E 是 (F,T) 的一个有限生成实扩张. 由于 (F,T) 是强局部稠密的, 从而 E 有一个包含 T 的正锥 Q_E, 且有 $a\in F$, 使得 $a\in]\alpha,\beta[_{Q_E}$. 令 $Q=Q_E\cap L$, 则 Q 为 L 的一个包含 T 的正锥.

又由于 $\alpha_i=(\sqrt{\alpha_i})^2\in Q_E\cap L=Q$, $i=1,\cdots,m$. 从而进一步有 $S\subseteq Q$. 此时, 显然 $a\in]\alpha,\beta[_Q$. 因此, (K,S) 是强局部稠密的. 证毕.

转换思考的角度, 自然会问: 若 (K,S) 是亚序域 (F,T) 的一个有限生成扩张, 且 (K,S) 具有弱 Hilbert 性质, 亚序域 (F,T) 是否一定具有弱 Hilbert 性质? 这一问题可看做弱 Hilbert 性质对于亚序域的有限生成扩张的下降问题. 下面将看到, 这个下降问题的回答在一般情况下是否定的.

定义 4.6.3 亚序域 (F,T) 的一个自然扩张 是指一个亚序域 (K,S), 使得 K 是 F 的一个域扩张, 同时 $S=\left\{\sum_{i=1}^{n}t_i\alpha_i^2 \mid n\text{为自然数}, t_i\in T, \alpha_i\in K, i=1,\cdots,n\right\}$.

现在, 我们可建立下面的结果.

定理 4.6.5 设 (K,S) 是亚序域 (F,T) 的一个自然扩张, 则当 K 是 F 的一个

纯超越扩张时，(K,S) 具有弱 Hilbert 性质.

证明　由条件可设 $K=F(B)$, 其中 B 是 K 在 F 上的一个超越基. 为证明 (K,S) 具有弱 Hilbert 性质，由定理 4.4.5 的推论 1 知，只须证明：(K,S) 上每个非强半正定的单元多项式同时也不是半正定的. 现设 $g(x)\in K[x]$ 在 (K,S) 上不是强半正定的，即对于 (K,S) 的某个实闭包 R_K 以及某个 $\eta\in R_K$, $g(\eta)<_{R_K^2}0$. 为证明 $g(x)$ 在 (K,S) 上不是半正定多项式，我们就 K 在 F 上的超越次数 $|B|$ 分三种情况进行讨论.

情况 1　$|B|=1$. 此时，可设 $B=\{\xi\}$. 由于 $g(x)\in F(\xi)[x]$, 从而 $g(x)$ 可改写成：$g(x)=f(\xi,x)$, 这里 $f(\xi,x)$ 是 F 上一个含未定元 ξ, x 的有理函数. 于是 $f(\xi,\eta)<_{R_K^2}0$. 令 $P=R_K\cap F$, 且 R 是序域 (F,P) 的实闭包. 由 Lang 同态定理知，对于某两个 $\alpha,\beta\in R$, 有 $f(\alpha,\beta)<_{R^2}0$.

由熟知的本原元定理，有 $\theta\in F(\alpha,\beta)$, 使得 $F(\alpha,\beta)=F(\theta)$. 由于 θ 是 F 上的代数元，从而由引理 1.2.2 知，有 $a\in F$, 使得 $|\theta|_{R^2}<_{R^2}a$. 此外，由引理 4.4.3 知，有 $\delta\in S_F$, 使得对于 $y,z\in R$, 只要 $|y-\alpha|_{R^2}<_{R^2}\delta$ 且 $|z-\beta|_{R^2}<_{R^2}\delta$, 必有 $f(y,z)<_{R^2}0$.

考察 F 和 $F(\theta)$ 之间诸如 $F(\alpha+\frac{1}{n}a^{-1}\theta\delta)$ $(n\in\mathbb{N})$ 的中间域. 由于 F 和 $F(\theta)$ 之间仅有有限个中间域, 从而有 $r,s\in\mathbb{N}$, 使得 $r\neq s$, 且 $F(\alpha+\frac{1}{r}a^{-1}\theta\delta)=F(\alpha+\frac{1}{s}a^{-1}\theta\delta)$. 此时易知，$F(\theta)=F(\gamma)$, 其中 $\gamma=\alpha+\frac{1}{r}a^{-1}\theta\delta$. 于是 $\beta\in F(\gamma)$, 即 $\beta=h(\gamma)$, 这里 $h(x)\in F[x]$. 注意到 $|\gamma-\alpha|_{R^2}=|\frac{1}{r}a^{-1}\theta\delta|_{R^2}<_{R^2}\delta$. 从而 $f(\gamma,h(\gamma))<_{R^2}0$.

设 Q 是域 $R(\xi)$ 的这样一个正锥，使得 $\xi-\gamma$ 在 R 上是正的无穷小元素. 于是 $f(\gamma+(\xi-\gamma),h(\gamma+(\xi-\gamma)))<_Q 0$, 即 $f(\xi,h(\xi))<_Q 0$. 令 $P=Q\cap K$. 显然有 $S\subseteq P$, 即 P 是亚序域 (K,S) 的一个序. 此时，有 $f(\xi,h(\xi))<_P 0$, 即 $g(h(\xi))<_P 0$. 因此，$g(x)$ 在 (K,S) 上不是半正定的.

情况 2　$|B|=m>1$. 此时，可设 $B=\{\xi_1,\cdots,\xi_m\}$. 令 $K_1=F(\xi_1)$, 且 $S_1=\left\{\sum_{i=1}^{n}t_i\alpha_i^2 \mid n\text{为自然数}, t_i\in T, \alpha_i\in K_1, i=1,\cdots,n\right\}$. 由情况 1 的证明，$(K_1,S_1)$ 具有弱 Hilbert 性质. 注意到 (K,S) 是 (K_1,S_1) 的一个有限生成扩张. 从而由定理 4.6.4 知，(K,S) 具有弱 Hilbert 性质.

情况 3　$|B|=\infty$. 由于 $g(x)\in F(B)[x]$, 从而存在有限多个元素 $\xi_1,\cdots,\xi_m\in B$, 使得 $g(x)\in F(\xi_1,\cdots,\xi_m)[x]$, 且 η 在 $F(\xi_1,\cdots,\xi_m)$ 上是代数的. 令 $Q=R_K\cap F(\xi_1,\cdots,\xi_m,\eta)$, 则 $g(\eta)<_Q 0$. 换句话说，$g(x)$ 在 (K_1,S_1) 上不是强半正定的, 这里 $K_1:=F(\xi_1,\cdots,\xi_m)$, 而 $S_1:=\left\{\sum_{i=1}^{n}t_i\alpha_i^2 \mid n\text{为自然数}, t_i\in T, \alpha_i\in K_1, i=1,\cdots,n\right\}$.

由情况 2 的证明知，(K_1,S_1) 具有弱 Hilbert 性质, 从而 $g(x)$ 在 (K_1,S_1) 上不是半正定

的. 于是, 对于 (K_1, S_1) 的某个序 P_1 以及某个 $u \in K_1$, $g(u) <_{P_1} 0$. 由于 K 是 K_1 的一个纯超越扩张, 从而易知 $S_2 := \left\{\sum_{i=1}^{n} p_i\alpha_i^2 \mid n\text{为自然数}, p_i \in P_1, \alpha_i \in K, i = 1, \cdots, n\right\}$ 是 K 的一个亚正锥. 因而, K 有一个正锥 P, 使得 $S_2 \subseteq P$. 显然 $S \subseteq S_2$, 且 $P_1 \subseteq S_2$. 从而 P 是 (K, S) 的一个正锥, 且 $g(u) <_P 0$, 这里 $u \in K$. 因此, $g(x)$ 在 (K, S) 上不是半正定的. 至此定理获证.

由定理 4.6.5 , 我们容易得到下面的定理.

定理 4.6.6 设 (K, S) 是亚序域 (F, T) 的一个有限生成扩张, 则当 K 是 F 的超越扩张时, 亚序域 (K, S) 具有弱 Hilbert 性质.

证明 在 K 中任取一个在 F 上超越的元素 ξ, 且令 $K_1 = F(\xi)$, 而 $S_1 = \left\{\sum_{i=1}^{n} t_i\alpha_i^2 \mid n\text{为自然数}, t_i \in T, \alpha_i \in K_1, i = 1, \cdots, n\right\}$. 于是 (K_1, S_1) 是 (F, T) 的一个自然扩张. 由定理 4.6.5 知, 亚序域 (K_1, S_1) 具有弱 Hilbert 性质. 注意到 (K, S) 是 (K_1, S_1) 的一个有限生成扩张, 从而由定理 4.6.4 即可得结论.

在定理 4.6.6 中, 尽管 (K, S) 具有弱 Hilbert 性质, 但 (F, T) 却未必. 这就否定地回答了前面的问题.

鉴于定理 4.6.6, 自然会问: 如果进一步假设 K 在 F 上是代数的, 上述问题是否有肯定的回答? 事实上, 回答仍是否定的. 对此, 参见下面的反例.

反例 设 $F = \mathbb{Q}(t)$, 这里 t 是有理数域 $\mathbb{Q}$ 上的一个未定元, 则 K 至少有这样的两个正锥 P_1 和 P_2, 使得如下条件成立: 对于 P_1, t 在 $\mathbb{Q}$ 上是正的无穷小元素; 而关于 P_2, $f(t) \in P_2$ 当且仅当 $f(\pi) \geqslant 0$, 这里 $f(t) \in \mathbb{Q}(t)$, 而 $\pi = 3.1415\cdots$ 是通常的圆周率 (超越实数). 令 $T = P_1 \cap P_2$.

设 P 是亚序域 (F, T) 的任意正锥. 假若 $P \neq P_1$ 且 $P \neq P_2$, 则有 $a, b \in P$, 使得 $a \notin P_1$ 且 $b \notin P_2$. 由于 $T \subseteq P$, 从而易知 $-a \notin P_2$ 且 $-b \notin P_1$, 即 $a \in P_2$ 且 $b \in P_1$. 由此有 $-ab \in P_1 \cap P_2$, 即有 $ab \in P \cap -P$. 于是 $ab = 0$, 即 $a = 0$ 或 $b = 0$, 矛盾. 因而, 亚序域 (F, T) 恰有两个正锥 P_1 和 P_2.

再令 $K = F(\sqrt{t-1})$, 而 $S = \left\{\sum_{i=1}^{n} t_i\alpha_i^2 \mid n\text{为自然数}, t_i \in T, \alpha_i \in K, i = 1, \cdots, n\right\}$. 由同构关系 $K \cong \mathbb{Q}(\sqrt{\pi - 1})$, 易知 $-1 \notin S$. 于是 (K, S) 是 (F, T) 的一个有限生成扩张, 且 K 显然是 F 的代数扩张. 对于 (K, S) 的任意正锥 Q, 必有 $t - 1 = (\sqrt{t-1})^2 \in Q$, 从而 $t - 1 \in Q \cap F$. 此时有 $Q \cap F = P_2$. 由于 P_2 是域 F 的一个阿基米德正锥, 且 K 是 F 的代数扩张. 从而 Q 是 K 的一个阿基米德正锥. 因而, 亚序域 (K, S) 的每个序都是阿基米德的, 自然 (K, S) 具有弱 Hilbert 性质. 然而, F 在序域 (F, P_1) 的实闭包中不稠密. 从而由定理 4.3.1 知, 亚序域 (F, T) 不具有弱 Hilbert 性质.

在上面的反例中，若改令 $K = F(\sqrt{1-t})$, 则易知 (K,S) 的每个正锥都是 P_1 在 K 上的拓展. 于是，对于 (K,S) 的任意正锥 Q, 我们有如下两种情况： (i) 当 $\sqrt{1-t} \in Q$ 时，对于每个正有理数 q, $0 <_Q 1 - \sqrt{1-t} = \dfrac{t}{1+\sqrt{1-t}} <_Q t <_Q q$; 或者 (ii) 当 $-\sqrt{1-t} \in Q$ 时，对于每个正有理数 q, $0 <_Q 1 + \sqrt{1-t} = \dfrac{t}{1-\sqrt{1-t}} <_Q t <_Q q$. 注意到 $K = \mathbb{Q}(1+\sqrt{1-t}) = \mathbb{Q}(1-\sqrt{1-t})$. 从而 K 在序域 (K,Q) 的实闭包中不稠密. 同样，由定理 4.3.1 知， (K,S) 不具有弱 Hilbert 性质. 这一事实说明了，在定理 4.6.6 中，条件 "K 是 F 的超越扩张" 并非多余.

然而，如果仅考虑序域的有限亚序扩张，则前面的问题有肯定的回答. 事实上，借助于定理 4.5.4, 我们可以获得下面的定理.

定理 4.6.7 设 (F,P) 是一个序域，且 (K,S) 是一个亚序域，使得 K 是 F 的一个有限扩张，同时 $P \subseteq S$, 则 (F,P) 具有弱 Hilbert 性质，当且仅当 (K,P) 具有弱 Hilbert 性质.

证明 设 Q 是 (K,S) 的任意一个序，且 R 是序域 (K,Q) 的实闭包，则 R 也是序域 (K,P) 的实闭包.

现设 (F,P) 具有弱 Hilbert 性质. 由定理 4.2.4 知， F 在 R 中稠密，因而 K 在 R 中稠密. 因此， K 在 (K,S) 的每个实闭包中都是稠密的，自然 (K,S) 具有弱 Hilbert 性质.

反过来，设 (K,S) 具有弱 Hilbert 性质. 很清楚，正锥 P 在 K 上仅有有限多个拓展，因为 K 是 F 的有限扩张. 因而，亚序域 (K,S) 只有有限个多个序. 由定理 4.3.1 知， K 在 R 中稠密. 不失一般性，可假定 P 是 F 的一个非阿基米德正锥；否则 (F,P) 已经具有弱 Hilbert 性质. 对于域 F 的每个与 P 相容的非浅显赋值 v, 由定理 3.2.5 知，至少有 K 的一个赋值 w, 使得 w 是 v 的一个拓展，且 w 与 Q 相容. 用 G_v 和 F_v (或 G_w 和 F_w) 依次表示 v (或 w) 的值群和剩余域. 根据定理 4.5.4, G_w 是可除的，且 F_w 是实闭的. 由赋值论的一个熟知结论，商群 G_w/G_v 是一个有限群，且 F_w 是 F_v 的一个有限扩张. 用 m 表示群 G_w/G_v 的阶. 由于 G_w 是可除的，从而对于任意 $g \in G_w$, 有 $h \in G_w$, 使得 $g = mh$. 此时有 $g = mh \in G_v$. 因而 $G_v = G_w$. 此外，由定理 2.2.1, 有 $F_v = F_w$. 再由定理 4.5.4 知， F 在 R 中稠密. 因此， (F,P) 具有弱 Hilbert 性质. 证毕.

推论 设 (K,Q) 是序域 (F,P) 的一个有限序扩张，则 (F,P) 具有弱 Hilbert 性质，当且仅当 (K,Q) 具有弱 Hilbert 性质.

有例子表明这样一个事实：倘若将上面推论中的条件 "K 是 F 的一个有限扩张" 减弱为： "K 在 F 上是有限生成的", 则结论不复成立. 对此感兴趣的读者可参见文献 [205].

第五章　实域上二次型与半序

在前面的讨论中，无论是域的实性还是 Hilbert 第十七问题，许多问题都涉及域中元素的这样一类表示形式：平方和或者带有特定系数的平方和. 实际上，这样一类平方和形式都可看作域上相应二次型的值. 因此，这一事实决定了实域理论和二次型理论之间的自然联系.

在本章中，我们将从二次型的基本概念出发，建立一些与实域有关的重要结果. 在这些重要的结果中，有从定量方面回答 Hilbert 第十七问题的 Cassels 定理和 Pfister 定理. 此外，在实域上还引进一种与二次型密切相关的序关系 — 半序. 半序在条件上弱于“序”这一概念，然而一些适合序的结论对于半序也成立.

§5.1　域上二次型

在本节中，将介绍二次型理论中的一些基本概念和本书所需的有关结论. 在本节和以后各节中，所涉及的域的特征均不为 2, 今后不再特别说明.

设 F 是一个域. 域 F 上的一个 n 元二次型是如下 F 上 n 元二次齐次多项式：

$$q := q(x_1, \cdots, x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_ix_j,$$

其中 $x_1, \cdots, x_n$ 是域 F 上 n 个未定元，$a_{ij} \in F$, 且 $a_{ij} = a_{ji}$, $i, j = 1, \cdots, n$. 域 F 上的一个 n 元二次型 q 常简称作 F 上的一个 n 维型，而自然数 n 称作该二次型的维数，且记作 $\dim(q) = n$.

如上二次型 q 惟一地对应域 F 上的对称矩阵 $A = (a_{ij})_{n\times n}$, 使得

$$q(x_1, \cdots, x_n) = (x_1, \cdots, x_n)A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

这个矩阵 A 称作二次型 q 的矩阵, 矩阵 A 的秩也称作二次型 q 的秩, 且记作 $\mathrm{rank}(q)$.

通过域 F 上一个关于变量的非退化线性替换，F 上一个二次型 q 可化成一个新的二次型 ϱ, 使得 $C^{\mathrm{T}}AC = B$, 其中 A 和 B 分别为 q 和 ϱ 的矩阵，C 是所给的非退化线性替换的系数矩阵，且 C^{T} 表示矩阵 C 的转置.

定义 5.1.1　称域 F 上二次型 q 和 ϱ 在 F 上合同，若通过 F 上某个非退化的线性替换，q 可化成 ϱ. 此时记作 $q \approx_F \varrho$.

由定义知，$q \approx_F \varrho$, 当且仅当有 F 上可逆矩阵 C, 使得 $C^{\mathrm{T}}AC = B$, 其中 A 和 B 分别为 q 和 ϱ 的矩阵. 此时，亦称矩阵 A 和 B 在 F 上合同，且记作 $A \approx_F B$. 当 $q \approx_F \varrho$ 时，显然有 $\dim(q) = \dim(\varrho)$, 且 $\operatorname{rank}(q) = \operatorname{rank}(\varrho)$. 很清楚，$\approx_F$ 是 F 上二次型 (对称矩阵) 之间的一个等价关系. 关于 $\approx_F$, 二次型的等价类称作合同类.

只含平方项的型 $\sum\limits_{i=1}^{n} a_i x_i^2$ 简记作 $\langle a_1, \cdots, a_n\rangle$. 作为二次型理论中一个熟知事实，我们有如下的命题.

命题 5.1.1 域 F 上的每个 n 维型 q 都可对角化，即有 $a_1, \cdots, a_n \in F$, 使得 $q \approx_F \langle a_1, \cdots, a_n\rangle$.

根据上面命题，在二次型的每个合同类中，都可选取只含平方项的二次型作为其代表. 对于 F 上一个型 q, 若 $q \approx_F \langle a_1, \cdots, a_n\rangle$, 则称 $\langle a_1, \cdots, a_n\rangle$ 是型 q 的一个标准形.

设 $q := q(x_1, \cdots, x_n)$ 是域 F 上的一个 n 维型，K 是 F 的一个域扩张 (可能 $K = F$), 则 q 显然可作为 K 上的一个型. 令 $K^n := \{(a_1, \cdots, a_n) \mid a_i \in K, i = 1, \cdots, n\}$ 是域 K 上 n 维行向量空间，且对于 $u = (a_1, \cdots, a_n) \in K^n$, 记 $q(u) = q(a_1, \cdots, a_n)$. 于是，我们有一个集合 $D_K(q) = \{q(u) \mid u \in K^n, 且\ q(u) \neq 0\}$. 若 $d \in D_K(q)$, 则称 d 在 K 上可被 q 表示. 显然，当 $q \approx_K \varrho$ 时，有 $D_K(q) = D_K(\varrho)$. 此外，若 $d \in D_K(q)$, 即对于某个 $u \in K^n$ (n 为型 q 的维数), $d = q(u)$, 则 $d^{-1} = d^{-2}q(u) = q(d^{-1}u) \in D_K(q)$.

命题 5.1.2 设 q 是域 F 上的一个 n 维型，且 $d \in \dot{F}$, 则 $d \in D_F(q)$, 当且仅当有 $b_2, \cdots, b_n \in F$, 使得 $q \approx_F \langle d, b_2, \cdots, b_n\rangle$.

证明 充分性：设 $q \approx_F \varrho = \langle d, b_2, \cdots, b_n\rangle$, 其中 $b_2, \cdots, b_n \in F$, 则 $d = d \cdot 1^2 + b_2 \cdot 0^2 + \cdots + b_n \cdot 0^2 \in D_F(\varrho) = D_F(q)$.

必要性：设 $d \in D_F(q)$, 且不妨令 $q = \langle a_1, \cdots, a_n\rangle$, 则有 $d = a_1c_1^2 + \cdots + a_nc_n^2$, 这里 $c_1, \cdots, c_n \in F$. 由于 $d \neq 0$, 从而 $c_1, \cdots, c_n$ 不全为 0. 不妨设 $c_1 \neq 0$.

记 A 为型 $\langle a_2, \cdots, a_n\rangle$ 的矩阵，$u = (c_2, \cdots, c_n)$, 且 I 为 F 上的 $n-1$ 阶单位矩阵，则由分块矩阵的计算可得

$$B\begin{pmatrix} a_1 & 0 \\ 0 & A \end{pmatrix}B^{\mathrm{T}} = \begin{pmatrix} d & 0 \\ 0 & A - d^{-1}Au^{\mathrm{T}}uA \end{pmatrix}.$$

其中

$$B = \begin{pmatrix} 1 & 0 \\ -d^{-1}Au^{\mathrm{T}} & I \end{pmatrix}\begin{pmatrix} c_1 & u \\ 0 & I \end{pmatrix}.$$

由于 $A - d^{-1}Au^{\mathrm{T}}uA$ 是 F 上的 $n-1$ 阶对称矩阵，从而有 F 上的 $n-1$ 阶可逆矩阵 C_1, 使得

$$C_1^{\mathrm{T}}(A-d^{-1}Au^{\mathrm{T}}uA)C_1=\begin{pmatrix} b_2 & & \\ & \ddots & \\ & & b_n \end{pmatrix}.$$

其中 $b_2,\cdots,b_n\in F$. 由此有

$$\begin{pmatrix} 1 & 0 \\ 0 & C_1^{\mathrm{T}} \end{pmatrix}\begin{pmatrix} d & 0 \\ 0 & A-d^{-1}Au^{\mathrm{T}}uA \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & C_1 \end{pmatrix}=\begin{pmatrix} d & & & \\ & b_2 & & \\ & & \ddots & \\ & & & b_n \end{pmatrix}.$$

注意到，诸矩阵

$$\begin{pmatrix} c_1 & 0 \\ u^{\mathrm{T}} & I \end{pmatrix},\begin{pmatrix} 1 & -d^{-1}uA \\ 0 & I \end{pmatrix},\begin{pmatrix} 1 & 0 \\ 0 & C_1 \end{pmatrix}$$

都是可逆的. 因此，$q\approx_F\langle d,b_2,\cdots,b_n\rangle$. 证毕.

定义 5.1.2 设 q 是域 F 上的一个 n 维型. 若有 $\dim(q)=rank(q)$, 则称 q 是正则的 .

定义 5.1.3 设 q 是域 F 上的一个正则 n 维型. 若有一个非零向量 $u\in F^n$, 使得 $q(u)=0$, 则称 q 在 F 上是迷向的; 否则，称 q 在 F 上是反迷向的.

从定义可知，迷向型的维数必定大于 1. 此外，易知当 $q\approx_F\varrho$ 时，q 成为迷向的，当且仅当 ϱ 是迷向的. 对于迷向型，我们还有如下的命题.

命题 5.1.3 对于域 F 上的 n 维迷向型 q, 有以下的论断成立:

(1) 存在 $b_3,\cdots,b_n\in\dot{F}$, 使得 $q\approx_F\langle 1,-1,b_3,\cdots,b_n\rangle$.

(2) $D_F(q)=\dot{F}$.

证明 不失一般性，可设 $q=\langle a_1,\cdots,a_n\rangle$, 其中 $n\geqslant 2$, $a_1,\cdots,a_n\in\dot{F}$.

(1) 此时，有非零向量 $(c_1,\cdots,c_n)\in F^n$, 使得 $a_1c_1^2+\cdots+a_nc_n^2=0$. 不妨设 $c_1\neq 0$, 于是 $-a_1=a_2\left(\dfrac{c_2}{c_1}\right)^2+\cdots+a_n\left(\dfrac{c_n}{c_1}\right)^2\in D_F(\langle a_2,\cdots,a_n\rangle)$. 按命题 5.1.2, 应有 $\langle a_2,\cdots,a_n\rangle\approx_F\langle -a_1,b_3,\cdots,b_n\rangle$, 其中 $b_3,\cdots,b_n\in\dot{F}$. 注意到,

$$C^{\mathrm{T}}\begin{pmatrix} a_1 & \\ & -a_1 \end{pmatrix}C=\begin{pmatrix} 1 & \\ & -1 \end{pmatrix},$$

其中 $C=\dfrac{1}{2}\begin{pmatrix} 1+a_1^{-1} & a_1^{-1}-1 \\ a_1^{-1}-1 & 1+a_1^{-1} \end{pmatrix}$ 为 F 上的可逆矩阵. 从而可得，$q\approx_F\langle a_1,-a_1,b_3,\cdots,b_n\rangle\approx_F\langle 1,-1,b_3,\cdots,b_n\rangle$.

(2) 设 $d \in \dot{F}$, 则由论断 (1) 有，$d = \left(\frac{1+d}{2}\right)^2 - \left(\frac{1-d}{2}\right)^2 + b_3 \cdot 0^2 + \cdots + b_n \cdot 0^2 \in D_F(\langle 1, -1, b_3, \cdots, b_n\rangle) = D_F(q)$. 证毕.

对于满足 $D_F(q) = \dot{F}$ 的型 q, q 称作在 F 上是泛的. 由命题 5.1.3(1) 的证明可见，下面的事实成立.

推论 对于域 F 上的 2 维型 $q = \langle b, c\rangle$, 下面的叙述等价:

(1) q 是迷向的;

(2) 对于某个 $a \in \dot{F}$, $q \approx_F \langle a, -a\rangle$;

(3) $q \approx_F \langle 1, -1\rangle$;

(4) $-bc \in \dot{F}^2$.

证明 由命题 5.1.3(1) 的证明知, 蕴含关系 "(1) $\Longrightarrow$ (2) $\Longrightarrow$ (3)" 成立. 显然, 蕴含关系 "(3) $\Longrightarrow$ (1)" 也成立.

"(1) $\Longleftrightarrow$ (4)": 设 q 是迷向的, 则 b 和 c 全不为零, 且有不全为零的 $d, e \in F$, 使得 $bd^2 + ce^2 = 0$. 此时, 显然 d 和 e 全不为零. 由此有 $-bc = (ced^{-1})^2 \in \dot{F}^2$. 反过来, 若 $-bc \in \dot{F}^2$, 则对于某个 $d \in \dot{F}$, $-bc = d^2$. 从而 $bc^2 + cd^2 = 0$. 这表明 q 是迷向的. 证毕.

命题 5.1.4(Springer) 设 K 是域 F 的一个奇次数扩张, $\langle a_1, \cdots, a_n\rangle$ 是 F 上一个型, 其中 $a_1, \cdots, a_n \in \dot{F}$, 则 $\langle a_1, \cdots, a_n\rangle$ 在 F 上是反迷向的, 当且仅当 $\langle a_1, \cdots, a_n\rangle$ 在 K 上是反迷向的.

证明 充分性显然. 假若命题的必要性不成立, 则由自然数的良序性, 可选取这样的奇次数扩张 $F \subseteq K$, 使得 (i)$\langle a_1, \cdots, a_n\rangle$ 在 F 上是反迷向的, 但在 K 上是迷向的; (ii) 在保证条件 (i) 成立的前提下, 扩张次数 $[K : F]$ 最小.

取 $\alpha \in K$, 使得 $\alpha \notin F$. 由 F 和 K 的选取可知, $K = F(\alpha)$. 令 $m = [K : F]$, 且设 $g(x)$ 是 α 在 F 上的极小多项式. 由于 $\langle a_1, \cdots, a_n\rangle$ 在 K 上是迷向的, 从而根据单代数扩张 $K = F(\alpha)$ 中的元素形式知, 存在 F 上次数不超过 $m - 1$ 的多项式 $f_i(x)$, $i = 1, \cdots, n$, 使得 $f_1(x), \cdots, f_n(x)$ 没有非常量公因式, 且有

$$\sum_{i=1}^{n} a_i f_i(\alpha)^2 = 0.$$

从而, 对于 $F[x]$ 中某个多项式 $h(x)$, $\sum_{i=1}^{n} a_i f_i(x)^2 = g(x)h(x)$.

由于 $\langle a_1, \cdots, a_n\rangle$ 在 F 上是反迷向的, 从而可知 $\sum_{i=1}^{n} a_i f_i(x)^2$ 是 F 上一个偶次数的多项式, 且其次数不大于 $2(m-1)$. 于是, $h(x)$ 的次数是一个小于 m 的奇数. 因此, $h(x)$ 在 $F[x]$ 中至少有一个奇次数的不可约因式 $p(x)$. 令 β 是 $p(x)$ 在

F 的代数闭包中的一个根，则 $\sum_{i=1}^{n} a_i f_i(\beta)^2 = 0$. 由于 $f_1(x), \cdots, f_n(x)$ 没有非常量公因式，从而 $f_1(\beta), \cdots, f_n(\beta)$ 不全为零. 因而 $\langle a_1, \cdots, a_n\rangle$ 在 $F(\beta)$ 上是迷向的. 然而，$[F(\beta):F]$ 显然是一个小于 $[K:F]$ 的奇数，这矛盾于 F 和 K 的选取，从而定理获证.

命题 5.1.5 对于域 F 上的两个 2 维正则型 $q = \langle a_1, a_2\rangle$ 和 $\varrho = \langle b_1, b_2\rangle$, $q \approx_F \varrho$ 当且仅当 $b_1 \in D_F(q)$, 且 $a_1a_2b_1b_2 \in \dot{F}^2$.

证明 若 $q \approx_F \varrho$, 则 $b_1 = b_1 \cdot 1^2 + b_2 \cdot 0^2 \in D_F(\varrho) = D_F(q)$, 且有 F 上可逆矩阵 C, 使得

$$C^{\mathrm{T}} \begin{pmatrix} a_1 & \\ & a_2 \end{pmatrix} C = \begin{pmatrix} b_1 & \\ & b_2 \end{pmatrix}.$$

两边取行列式，即有 $a_1a_2(\det(C))^2 = b_1b_2$, 这里 $\det(C)$ 表示矩阵 C 的行列式. 从而 $a_1a_2b_1b_2 = (a_1a_2\det(C))^2 \in \dot{F}^2$.

反之，若 $b_1 \in D_F(q)$, 且 $a_1a_2b_1b_2 = d^2$, 其中 $d \in \dot{F}$, 则由命题 5.1.2，有 $c \in \dot{F}$, 使得 $\langle a_1, a_2\rangle \approx_F \langle b_1, c\rangle$. 由必要性的证明，我们有 $a_1a_2b_1c = e^2$, 其中 $e \in \dot{F}$. 这样，$c = b_2(ed^{-1})^2$. 从而 $\langle b_1, c\rangle \approx_F \langle b_1, b_2\rangle$, 故 $\langle a_1, a_2\rangle \approx_F \langle b_1, b_2\rangle$. 证毕.

现在，我们对 F 上的型来规定两个运算：直和 $\oplus$ 与张量积 $\otimes$. 设 q 和 ϱ 是 F 上的两个型，且 $A = (a_{ij})_{n\times n}$ 和 $B = (b_{ij})m \times m$ 分别为 q 和 ϱ 的矩阵. 今规定 F 上两个二次型 $q \oplus \varrho$ 和 $q \otimes \varrho$, 使得它们的矩阵依次为如下分块矩阵：

$$\begin{pmatrix} A & \\ & B \end{pmatrix}, \quad (a_{ij}B)_{n\times n} = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nn}B \end{pmatrix}.$$

为讨论的需要，有必要再引进一个附加的符号 0, 且规定：对于域 F 上的每个型 q, $q \oplus 0 = q$, 且 $q \otimes 0 = 0$. 此时，我们称符号 0 是域 F 上的 0 维型.

命题 5.1.6 设 q, q_1, ϱ 和 ϱ_1 都是 F 上的型，且 $q \approx_F q_1$, $\varrho \approx_F \varrho_1$, 则有 $q \oplus \varrho \approx_F q_1 \oplus \varrho_1$ 以及 $q \otimes \varrho \approx_F q_1 \otimes \varrho_1$.

证明 设 $A = (a_{ij})_{n\times n}$, $A_1 = (\alpha_{ij})_{n\times n}$, $B = (b_{ij})_{m\times m}$ 和 $B_1 = (\beta_{ij})_{m\times m}$ 分别为 q, q_1, ϱ 和 ϱ_1 的矩阵，则存在 F 上 n 阶可逆矩阵 $C = (c_{ij})_{n\times n}$ 和 m 阶可逆矩阵 E, 使得

$$C^{\mathrm{T}}AC = A_1, \quad 且\ E^{\mathrm{T}}BE = B_1.$$

由此有

$$\begin{pmatrix} C^{\mathrm{T}} & \\ & E^{\mathrm{T}} \end{pmatrix}\begin{pmatrix} A & \\ & B \end{pmatrix}\begin{pmatrix} C & \\ & E \end{pmatrix}=\begin{pmatrix} A_1 & \\ & B_1 \end{pmatrix},$$

且有

$$\begin{aligned}&\begin{pmatrix} E^{\mathrm{T}} & & \\ & \ddots & \\ & & E^{\mathrm{T}} \end{pmatrix}(c_{ij}I)^{\mathrm{T}}_{n\times n}(a_{ij}B)_{n\times n}(c_{ij}I)_{n\times n}\begin{pmatrix} E & & \\ & \ddots & \\ & & E \end{pmatrix}\\ =\ &(\alpha_{ij}B_1)_{n\times n},\end{aligned}$$

其中 I 是 F 上 m 阶单位矩阵.

显然,

$$\begin{pmatrix} C & \\ & E \end{pmatrix},\begin{pmatrix} E & & \\ & \ddots & \\ & & E \end{pmatrix}$$

都是域 F 上可逆矩阵. 再令 $C^{-1}=(d_{ij})_{n\times n}$. 通过直接验算可知, $(d_{ij}I)_{n\times n}$ 是 $(c_{ij}I)_{n\times n}$ 的逆矩阵. 因而, $(c_{ij}I)_{n\times n}$ 也是 F 上可逆矩阵. 因此, 命题获证.

推论 若 $q\approx_F\langle a_1,\cdots,a_n\rangle$, 且 $\varrho\approx_F\langle b_1,\cdots,b_m\rangle$, 则

$$q\oplus\varrho\approx_F\langle a_1,\cdots,a_n,b_1,\cdots,b_m\rangle$$
$$q\otimes\varrho\approx_F\langle a_1b_1,\cdots,a_1b_m,\cdots,a_nb_1,\cdots,a_nb_m\rangle.$$

由命题 5.1.6 及其推论可知, $\dim(q\oplus\varrho)=\dim(q)+\dim(\varrho)$, $\dim(q\otimes\varrho)=\dim(q)\cdot\dim(\varrho)$, $\mathrm{rank}(q\oplus\varrho)=\mathrm{rank}(q)+\mathrm{rank}(\varrho)$, 以及 $\mathrm{rank}(q\otimes\varrho)=\mathrm{rank}(q)\cdot\mathrm{rank}(\varrho)$.

命题 5.1.7 对于域 F 上的型 q, ϱ 和 σ, 我们有:

(1) (交换律) $q\oplus\varrho\approx_F\varrho\oplus q$; $q\otimes\varrho\approx_F\varrho\otimes q$;

(2) (结合律) $(q\oplus\varrho)\oplus\sigma\approx_F q\oplus(\varrho\oplus\sigma)$; $(q\otimes\varrho)\otimes\sigma\approx_F q\otimes(\varrho\otimes\sigma)$;

(3) (分配律) $(q\oplus\varrho)\otimes\sigma\approx_F(q\otimes\sigma)\oplus(\varrho\otimes\sigma)$.

命题 5.1.7 可通过命题 5.1.6 的推论而获得证明, 其证明要点是: 先化标准形, 再分别计算等式的两端. 作为练习, 建议读者自行验证上面命题. 命题 5.1.7 表明: 域 F 上二次型的所有合同类对于运算 $\oplus$ 和 $\otimes$ 是一个交换半环.

下面, 我们建立二次型理论中另一条基本定理 ——Witt 消去定理. 在证明 Witt 消去定理之前, 先证明下面的引理.

引理 5.1.8 设 q 和 ϱ 都是 F 上的型. 若 $\langle 0\rangle\oplus q\approx_F\langle 0\rangle\oplus\varrho$, 则有 $q\approx_F\varrho$.

证明 设 A 和 B 分别为 q 和 ϱ 的矩阵, 且 $n=\dim(q)$. 由所设, 有 F 上 $n+1$ 阶可逆矩阵

$$\begin{pmatrix} a & u \\ v^{\mathrm{T}} & C \end{pmatrix},$$

其中 u 和 v 都是 F 上 $1\times n$ 矩阵, 使得

$$\begin{pmatrix} a & v \\ u^{\mathrm{T}} & C^{\mathrm{T}} \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & A \end{pmatrix}\begin{pmatrix} a & u \\ v^{\mathrm{T}} & C \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & B \end{pmatrix}.$$

比较上式两端的对应矩阵块, 有 $vAv^{\mathrm{T}}=0$, $vAC=0$ 且 $C^{\mathrm{T}}AC=B$. 从而 $(aC-v^{\mathrm{T}}u)^{\mathrm{T}}A(aC-v^{\mathrm{T}}u)=a^2B$. 注意到, 矩阵 $aC-v^{\mathrm{T}}u$ 和矩阵

$$\begin{pmatrix} a & u \\ v^{\mathrm{T}} & C \end{pmatrix}$$

具有相同的行列式值, 于是, $aC-v^{\mathrm{T}}u$ 是可逆矩阵. 因此, $q\approx_F \varrho$. 证毕.

定理 5.1.9(Witt) 设 q, q_1, ϱ 和 ϱ_1 都是 F 上的型. 若 $q\approx_F q_1$, 且 $q\oplus\varrho\approx_F q_1\oplus\varrho_1$, 则有 $\varrho\approx_F\varrho_1$.

证明 由命题 5.1.6, 可直接设 $q_1=q$. 由于 $\mathrm{rank}(q)+\mathrm{rank}(\varrho)=\mathrm{rank}(q\oplus\varrho)=\mathrm{rank}(q\oplus\varrho_1)=\mathrm{rank}(q)+\mathrm{rank}(\varrho_1)$, 从而 $\mathrm{rank}(\varrho)=\mathrm{rank}(\varrho_1)$. 同样, $\dim(\varrho)=\dim(\varrho_1)$. 令 $r=\mathrm{rank}(\varrho)=\mathrm{rank}(\varrho_1)$, 则有 $b_1,\cdots,b_r,c_1,\cdots,c_r\in\dot{F}$, 使得 $\varrho\approx_F\langle b_1,\cdots,b_r,0,\cdots,0\rangle$, 且 $\varrho_1\approx_F\langle c_1,\cdots,c_r,0,\cdots,0\rangle$. 由此有 $\langle 0,\cdots,0\rangle\oplus q\oplus\varrho_2\approx_F\langle 0,\cdots,0\rangle\oplus q\oplus\varrho_3$, 这里 $\varrho_2=\langle b_1,\cdots,b_r\rangle$ 和 $\varrho_3=\langle c_1,\cdots,c_r\rangle$ 都是 F 上的正则型. 由引理 5.1.8 知, $q\oplus\varrho_2\approx_F q\oplus\varrho_3$. 此时显然有, $\varrho\approx_F\varrho_1$, 当且仅当 $\varrho_2\approx_F\varrho_3$. 因而, 可进一步设 ϱ 和 ϱ_1 是 F 上正则型. 同理, 可设 q 也是正则的.

设 $q\approx_F\langle a_1,\cdots,a_m\rangle$, 则 $\langle a_1,\cdots,a_m\rangle\oplus\varrho\approx_F\langle a_1,\cdots,a_m\rangle\oplus\varrho_1$. 由归纳法原理, 不妨直接设 $\langle a\rangle\oplus\varrho\approx_F\langle a\rangle\oplus\varrho_1$.

设 A 和 B 分别为 ϱ 和 ϱ_1 的矩阵, 且 $n=\dim(\varrho)$. 由所设, 有 F 上 $n+1$ 阶可逆矩阵

$$\begin{pmatrix} b & u \\ v^{\mathrm{T}} & C \end{pmatrix},$$

其中 u 和 v 都是 F 上 $1\times n$ 矩阵, 使得

$$\begin{pmatrix} b & v \\ u^{\mathrm{T}} & C^{\mathrm{T}} \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix}\begin{pmatrix} b & u \\ v^{\mathrm{T}} & C \end{pmatrix}=\begin{pmatrix} a & 0 \\ 0 & B \end{pmatrix}.$$

比较上式两端的对应矩阵块, 有 $vAv^{\mathrm{T}}=a(1-b^2)$, $vAC=-abu$, 且 $C^{\mathrm{T}}AC+$

$au^{\mathrm{T}}u=B$. 令 z 是 F 中一个待定元素. 由计算有 $(C+zv^{\mathrm{T}}u)^{\mathrm{T}}A(C+zv^{\mathrm{T}}u)=B+a[z^2-(bz+1)^2]u^{\mathrm{T}}u$. 显然, 方程 $z^2-(bz+1)^2$ 在 F 中有解 $z=e$. 此时, $(C+ev^{\mathrm{T}}u)^{\mathrm{T}}A(C+ev^{\mathrm{T}}u)=B$. 由于 B 是可逆矩阵, 从而 $C+ev^{\mathrm{T}}u$ 是可逆的. 这表明 $\varrho\approx_F\varrho_1$. 证毕.

§5.2 Cassels 定理

在这一节中, 我们将建立重要的 Cassels 定理. 从 Cassels 定理, 可得到一个下界, 这个下界适合所有强半正定 n 元多项式的平方和表示中平方项个数. 首先, 证明下面的一个重要结论.

命题 5.2.1(Cassels-Pfister) 设 q 是域 F 上的一个型, x 是 F 上的超越元, 且 $p(x)$ 是 $F[x]$ 中的一个非零多项式. 若 $p(x)$ 在域 $F(x)$ 上能被 q 表示, 则 $p(x)$ 在 $F[x]$ 上也能被 q 表示.

证明 不妨设 $q=\langle a_1,\cdots,a_n\rangle$, 其中 $a_1,\cdots,a_n\in\dot{F}$. 若 q 在 F 上是迷向的, 则有非零向量 $(c_1,\cdots,c_n)\in F^n$, 使得 $a_1c_1^2+\cdots+a_nc_n^2=0$. 不妨设 $c_1\neq0$. 注意到 $p(x)=a_1g^2(x)-a_1h^2(x)$, 其中 $g(x)=\dfrac{1}{2}(a_1^{-1}p(x)+1)$, $h(x)=\dfrac{1}{2}(a_1^{-1}p(x)-1)\in F[x]$. 于是有

$$p(x)=a_1g^2(x)+a_2[c_1^{-1}c_2h(x)]^2+\cdots+a_n[c_1^{-1}c_nh(x)]^2.$$

此时, 结论成立. 以下设 q 在 F 上是反迷向的.

由所给的条件, 可以得到如下等式:

$$p(x)=a_1\left(\frac{f_1}{f_0}\right)^2+\cdots+a_n\left(\frac{f_n}{f_0}\right)^2,$$

其中 $f_i(x)\in F[x]$, $i=0,1,\cdots,n$; 且 $f_0(x)\neq0$.

此外, 我们还可以进一步假定: 在上面所选取的等式中, $f_0(x)$ 的次数 $\deg f_0$ 不可能更小. 我们只需要证明 $\deg f_0=0$.

假若 $\deg f_0>0$, 则由多项式的带余除法有

$$f_i(x)=g_if_0+r_i,\ i=1,\cdots,n,$$

其中 $g_i(x)$, $r_i(x)\in F[x]$, $r_i(x)=0$ 或者 $\deg r_i(x)<\deg f_0$, $i=1,\cdots,n$.

令 $B(X_0,X_1,\cdots,X_n;Y_0,Y_1,\cdots,Y_n)=-p(x)X_0Y_0+a_1X_1Y_1+\cdots+a_nX_nY_n$ 是 $F[x]$ 上的一个双线性型. 由上面等式, 有 $B(f_0,\cdots,f_n;f_0,\cdots,f_n)=0$.

记 $g_0=1$, $B_1=B(g_0,\cdots,g_n;g_0,\cdots,g_n)$, $B_2=B(f_0,\cdots,f_n;g_0,\cdots,g_n)$, 且令 $h_i=B_1f_i-2B_2g_i$, $i=0,1,\cdots,n$, 则

$$
\begin{aligned}
& B(h_0,\cdots,h_n;h_0,\cdots,h_n) \\
= & -4B_1B_2B(f_0,\cdots,f_n;g_0,\cdots,g_n)+4B_2^2B(g_0,\cdots,g_n;g_0,\cdots,g_n) \\
= & -4B_1B_2^2+4B_1B_2^2=0,
\end{aligned}
$$

此即

$$-p(x)h_0^2+a_1h_1^2+\cdots+a_nh_n^2=0. \qquad (\star)$$

此外，我们有

$$
\begin{aligned}
f_0h_0 &= B_1f_0^2-2B_2f_0 \\
&= \left(-p(x)+\sum_{i=1}^n a_ig_i^2\right)f_0^2-2\left(-p(x)f_0+\sum_{i=1}^n a_if_ig_i\right)f_0 \\
&= p(x)f_0^2+\sum_{i=1}^n a_i(f_0^2g_i^2-2f_0f_ig_i) \\
&= \sum_{i=1}^n a_if_i^2+\sum_{i=1}^n a_i(f_0^2g_i^2-2f_0f_ig_i) \\
&= \sum_{i=1}^n a_i(f_i-g_if_0)^2 \\
&= \sum_{i=1}^n a_ir_i^2.
\end{aligned}
$$

由于 $r_1(x),\cdots,r_n(x)$ 不全为 0, 从而可设 m 为其中非零多项式的最大次数. 再设 $r_i(x)$ 的 m 次项 x^m 系数为 b_i, $i=1,\cdots,n$, 则 $b_1,\cdots,b_n$ 不全为 0. 由于 q 在 F 上是反迷向的，从而 $\sum_{i=1}^n a_ir_i^2$ 的 $2m$ 次项系数为 F 中非零元 $\sum_{i=1}^n a_ib_i^2$. 于是 $f_0h_0\neq 0$, 并且 $\deg f_0+\deg h_0=2m$. 由于 $m<\deg f_0$, 从而 $\deg h_0<\deg f_0$.

然而，由上面等式 $(\star)$ 有

$$p(x)=a_1\left(\frac{h_1}{h_0}\right)^2+\cdots+a_n\left(\frac{h_n}{h_0}\right)^2.$$

这与 f_0 的取法矛盾，因此， $\deg f_0=0$. 证毕.

根据命题 5.2.1, 在定理 4.2.4 的推论 2 和定理 4.4.5 的推论 2 中，措辞"单元有理函数"都可改进为"单元多项式". 此外，由命题 5.2.1, 容易建立如下称作"代换原理"的结果.

推论 设 q 是域 F 上的一个型， $x_1,\cdots,x_m$ 是域 F 上 m 个未定元，且 $p(x_1,\cdots,x_m)$ 是 $F[x_1,\cdots,x_m]$ 中的一个非零多项式. 若多项式 $p(x_1,\cdots,x_m)$ 在域 $F(x_1,\cdots,x_m)$ 上能被 q 表示，则对于任意 $b_1,\cdots,b_m\in F$, 使得 $p(b_1,\cdots,b_m)$ 在 F 上也能被 q 表示，只要 $p(b_1,\cdots,b_m)\neq 0$.

证明　不妨设 $q=\langle a_1,\cdots,a_n\rangle$. 由命题 5.2.1 有

$$p(x_1,\cdots,x_m)=a_1f_1^2(x_1,\cdots,x_m)+\cdots+a_nf_n^2(x_1,\cdots,x_m),$$

其中 $f_i(x_1,\cdots,x_m)\in F(x_1,\cdots,x_{m-1})[x_m]$, $i=1,\cdots,n$.

用 $x_m=b_m$ 代入上式, 可得到

$$p(x_1,\cdots,x_{m-1},b_m)=a_1f_1^2(x_1,\cdots,x_{m-1},b_m)+\cdots+a_nf_n^2(x_1,\cdots,x_{m-1},b_m).$$

这表明: $F[x_1,\cdots,x_{m-1}]$ 中多项式 $p(x_1,\cdots,x_{m-1},b_m)$ 在 $F(x_1,\cdots,x_{m-1})$ 上能被 q 表示. 借助于归纳法, 即可完成证明.

应用上面的结果, 我们还可证明如下的命题.

命题 5.2.2　设 $q=\langle a_1,\cdots,a_n\rangle$ 是域 F 上的一个反迷向型, $n\geqslant 2$, 且 $\varrho=\langle a_2,\cdots,a_n\rangle$, 则对于 $d\in\dot{F}$, $d\in D_F(\varrho)$, 当且仅当 $d+a_1x^2\in D_{F(x)}(q)$, 其中 x 是 F 上的未定元.

证明　设 $d\in D_F(\varrho)$. 由命题 5.1.2 知, $\varrho\approx_F\langle d\rangle\oplus\varrho_1$, 此处 ϱ_1 是 F 上的一个 $n-2$ 维型. 于是, $q\approx_F\langle d,a_1\rangle\oplus\varrho_1$, 从而 $d+a_1x^2\in D_{F(x)}(\langle d,a_1\rangle\oplus\varrho_1)=D_{F(x)}(q)$.

反过来, 设 $d+a_1x^2\in D_{F(x)}(q)$. 由命题 5.2.1 有

$$d+a_1x^2=a_1f_1^2(x)+\cdots+a_nf_n^2(x),$$

其中 $f_1(x),\cdots,f_n(x)\in F[x]$.

设 m 是 $f_1(x),\cdots,f_n(x)$ 中的非零多项式的最高次数. 由于 q 在 F 上是反迷向的, 从而由命题 5.2.1 的证明中最后部分, 类似地可证明上面等式右端的多项式的次数为 $2m$. 于是 $2m=2$, 即 $m=1$. 从而可记 $f_1(x)=ax+b$, 其中 $a,b\in F$. 令 $c=b(1-a)^{-1}$, 若 $a\neq 1$; 或 $c=-b(1+a)^{-1}$, 若 $a=1$. 这样, $f_1(c)=ac+b=\pm c$. 将 $x=c$ 代入上面恒等式, 则有

$$d+a_1c^2=a_1(\pm c)^2+\sum_{i=2}^n f_i^2(c).$$

因此, $d=\sum\limits_{i=2}^n f_i^2(c)\in D_F(\varrho)$. 证毕.

推论　设 F 是一个域, 使得 -1 不是 F 中 $n-1$ 个元素的平方和, x 是 F 上的一个未定元. 若 $d\in\dot{F}$, 且 $d+x^2$ 是 $F(x)$ 中 n 个元素的平方和, 则 d 是 F 中 $n-1$ 个元素的平方和.

证明　按所设, n 维型 $q=\langle 1,1,\cdots,1\rangle$ 在 F 上是反迷向的. 由于 $d+x^2\in D_{F(x)}(q)$, 从而由命题 5.2.2, 可知 d 在 F 上能被 $n-1$ 维型 $\langle 1,\cdots,1\rangle$ 表示. 证毕.

从上面的推论, 我们容易证明以下的定理.

定理 5.2.3(Cassels) 设 F 是一个域, 使得 -1 不是 F 中 $n-1$ 个元素的平方和, 且 $x_1,\cdots,x_n$ 都是 F 上的未定元. 于是 $1+x_1^2+\cdots+x_n^2$ 不可能是域 $F(x_1,\cdots,x_n)$ 中 n 个元素的平方和.

证明 只需用归纳法证明: 当 $1\leqslant k\leqslant n$ 时, $1+x_1^2+\cdots+x_k^2$ 不可能是域 $F(x_1,\cdots,x_k)$ 中 k 个元素的平方和.

显然, $1+x_1^2$ 不是 $F(x_1)$ 中一个元素的平方, 即结论在 $n=1$ 时成立. 今假定 $1+x_1^2+\cdots+x_{k-1}^2$ 不是 $F(x_1,\cdots,x_{k-1})$ 中 $k-1$ 个元素的平方, 其中 $1\leqslant k-1\leqslant n-1$. 由于 -1 不是 F 中 $n-1$ 个元素的平方和, 从而由命题 5.2.1 的推论知, -1 也不是 $F(x_1,\cdots,x_{k-1})$ 中 $n-1$ 个元素的平方和, 当然更不是 $k-1$ 个元素的平方和. 由上面推论的逆否形式, $1+x_1^2+\cdots+x_k^2$ 不是 $F(x_1,\cdots,x_k)$ 中 k 个元素的平方和. 至此, 归纳法即告完成.

由于任何一个实域都满足定理 5.2.3 的条件, 从而我们立即得到

推论 1 设 F 是一个实域, 则 $1+x_1^2+\cdots+x_n^2$ 不可能是域 $F(x_1,\cdots,x_n)$ 中 n 个元素的平方和.

推论 2 设 (F,T) 是一个亚序域, 则 $1+x_1^2+\cdots+x_n^2$ 不可能表成如下形式:

$$1+x_1^2+\cdots+x_n^2=t_1f_1^2+\cdots+t_nf_n^2,$$

其中 $t_i\in T$, $f_i\in F(x_1,\cdots,x_n)$, $i=1,\cdots,n$.

证明 假若 $1+x_1^2+\cdots+x_n^2$ 可表为如上形式. 设 R 是 (F,T) 的一个实闭包, 则 $t_i\in R^2$, $i=1,\cdots,n$. 于是 $1+x_1^2+\cdots+x_n^2$ 是域 $R(x_1,\cdots,x_n)$ 中 n 个元素的平方和, 与上面的推论矛盾. 证毕.

上面推论 2 表明: 对于亚序域 (F,T) 上的所有强半正定 n 元多项式, 它们的(系数属于 T 的) 平方和表示中平方项个数以 $n+1$ 为一个下界.

定理 5.2.4 设 q 和 $\varrho=\langle b_1,\cdots,b_m\rangle$ 都是域 F 上反迷向的二次型, 则下面叙述等价:

(1) 对于 F 上某个型 σ, $q\approx_F\varrho\oplus\sigma$;

(2) 对于 F 的任意扩张 K, $D_K(\varrho)\subseteq D_K(q)$;

(3) 在有理函数域 $F(x_1,\cdots,x_m)$ 上, 其中 $x_1,\cdots,x_m$ 是 F 上 m 个未定元, $b_1x_1^2+\cdots+b_mx_m^2$ 可被 q 表示.

证明 蕴含关系 "(1) $\Longrightarrow$ (2) $\Longrightarrow$ (3)" 是显然的. 下面用归纳法证明蕴含 "(3) $\Longrightarrow$ (1)": 由命题 5.2.1 的推论知, 通过代换 $x_1=1$, $x_2=\cdots=x_m=0$, b_1 可被 q 表示. 由此有 $q\approx_F\langle b_1\rangle\oplus q_1$, 其中 q_1 是反迷向的. 于是由所设, $b_1x_1^2+(b_2x_2^2+\cdots+b_mx_m^2)$ 在域 $F(x_2,\cdots,x_m)(x_1)$ 上可被 $\langle b_1\rangle\oplus q_1$ 表示. 根据命题 5.2.2, $b_2x_2^2+\cdots+b_mx_m^2$ 在 $F(x_2,\cdots,x_m)$ 上可被 q_1 表示. 由归纳假定, 有 F 上某个型 σ, 使得 $q_1\approx_F\langle b_2,\cdots,b_m\rangle\oplus\sigma$. 因而, $q\approx_F\varrho\oplus\sigma$. 证毕.

§5.3 Pfister 型

在本节，我们考虑一类特殊的二次型 ——Pfister 型. Pfister 型具有引人注目的重要性质，从而这种型在二次型理论中占有重要的地位. A. Pfister 对这种型作了专门的研究，并且获得许多有趣的和有应用价值的结果.

定义 5.3.1 设 $a_1, \cdots, a_n \in \dot{F}$. F 上的型 $\langle 1, a_1\rangle \otimes \cdots \otimes \langle 1, a_n\rangle$ 称作域 F 上的一个 n 重 Pfister 型. 为论述方便计，我们约定，F 上的 0 重 Pfister 型为 $\langle 1\rangle$.

由定义 5.3.1 知，2^n 维型 $\langle 1, 1, \cdots, 1\rangle = \langle 1, 1\rangle \otimes \cdots \otimes \langle 1, 1\rangle$ 是 F 上的一个 n 重 Pfister 型. 显然，一个 n 重 Pfister 型是个 2^n 维正则型. 此外，由张量积的定义，每个 $n(>0)$ 重 Pfister 型 q 都可写作 $q = \langle 1\rangle \oplus \varrho$, 这里 ϱ 是个 $2^n - 1$ 维正则型.

在讨论 Pfister 型之前，为书写的方便，有必要再引进一个记号. 设 q 是域 F 上的一个型，$c \in \dot{F}$. 现规定 $cq = \langle c\rangle \otimes q$. 当 $q = \langle a_1, \cdots, a_n\rangle$ 时，$cq = \langle ca_1, \cdots, ca_n\rangle$.

定理 5.3.1 设 q 是域 F 上的一个 n 重 Pfister 型，则对于 $d \in D_F(q)$, 有 $q \approx_F dq$.

证明 对 n 施用归纳法. 当 $n = 0$ 时，$q = \langle 1\rangle$. 此时 $d = c^2$, $c \in \dot{F}$. 因此 $dq = \langle c^2\rangle \approx_F \langle 1\rangle = q$, 即定理在 $n = 0$ 时成立.

今设定理对于 $n-1$ 重 Pfister 型成立. 现在考察 n 重 Pfister 型 q. 此时，$q = q_1 \otimes \langle 1, a\rangle$, 这里 $a \in \dot{F}$, q_1 是 F 上的一个 $n-1$ 重 Pfister 型. 设 $d \in D_F(q)$. 由于 $q = q_1 \otimes (\langle 1\rangle \oplus < a >) \approx_F q_1 \oplus aq_1$, 从而 $d \in D_F(q_1 \oplus aq_1)$. 于是有 $b, c \in D_F(q_1) \cup \{0\}$, 使得 $d = b + ac$. 现在分三种情形讨论:

(1)$c = 0$. 此时 $d = b \in D_F(q_1)$. 由归纳假定，有 $dq = \langle d\rangle \otimes (q_1 \otimes \langle 1, a\rangle) \approx_F (\langle d\rangle \otimes q_1) \otimes \langle 1, a\rangle \approx_F q_1 \otimes \langle 1, a\rangle = q$.

(2)$b = 0$. 此时 $d = ac$. 按归纳假定，有 $dq = (\langle a\rangle \otimes \langle c\rangle) \otimes (q_1 \otimes \langle 1, a\rangle) \approx_F cq_1 \otimes \langle a, a^2\rangle \approx_F q_1 \otimes \langle 1, a\rangle = q$.

(3)b 与 c 都不为零. 此时 $d \in D_F(\langle b, ac\rangle)$. 由归纳假定，有 $q \approx_F q_1 \oplus aq_1 \approx_F bq_1 \oplus acq_1 \approx_F q_1 \otimes \langle b, ac\rangle$. 据命题 5.1.5, $\langle b, ac\rangle \approx_F \langle d, abcd\rangle$. 从而有 $q \approx_F q_1 \otimes \langle d, abcd\rangle \approx_F dq_1 \oplus dabcq_1 \approx_F dq_1 \oplus daq_1 \approx_F d(q_1 \otimes \langle 1, a\rangle) = dq$.

因此，在任何情况下，定理都成立.

推论 设 q 是域 F 上的一个 Pfister 型，则 $D_F(q)$ 对于 F 的乘法构成一个群.

证明 显然，$1 \in D_F(q)$. 由于 $D_F(q)$ 中元素的逆仍属于 $D_F(q)$, 因此只须证明: $D_F(q)$ 关于 F 的乘法是封闭的. 注意到，对于 F 上的任意一个型 σ 以及 $c \in \dot{F}$, 总有 $D_F(c\sigma) = cD_F(\sigma)$. 这样，对于每个 $d \in D_F(q)$, $dD_F(q) = D_F(dq) = D_F(q)$. 因而，推论成立.

定理 5.3.2 设 $q = \langle 1\rangle \oplus \varrho$ 是域 F 上的一个 n 重 Pfister 型，$n > 0$. 若 $b \in D_F(\varrho)$, 则 $q \approx_F \langle 1, b\rangle \otimes \sigma$, 此处 σ 是 F 上的一个 $n-1$ 重 Pfister 型.

证明 对 n 使用归纳法. 当 $n=1$ 时, $q=\langle 1,a\rangle$. 从而 $\varrho=\langle a\rangle$. 若 $b\in D_F(\varrho)$, 则 $b=ac^2$, 其中 $c\in \dot{F}$. 此时, $q=\langle 1,a\rangle\approx_F\langle 1,ac^2\rangle=\langle 1,b\rangle$. 从而, 定理在 $n=1$ 时成立.

今设定理对每个 $n-1$ 重 Pfister 型成立. 设 q 是一个 n 重 Pfister 型, 则 $q=q_1\otimes\langle 1,a\rangle$, 这里 q_1 是 F 上的一个 $n-1$ 重 Pfister 型. 令 $q_1=\langle 1\rangle\oplus\varrho_1$, 则 $q\approx_F\langle 1\rangle\oplus\varrho_1\oplus aq_1$. 由 Witt 消去定理有, $\varrho\approx_F\varrho_1\oplus aq_1$. 设 $b\in D_F(\varrho)$, 则 $b=b_1+ac$, 其中 $b_1\in D_F(\varrho_1)\cup\{0\}$, $c\in D_F(q_1)\cup\{0\}$. 同样, 分三种情况来讨论:

(1)$c=0$. 此时 $b=b_1\in D_F(\varrho_1)$. 由归纳假定, 存在 F 上的一个 $n-2$ 重 Pfister 型 q_2, 使得 $q_1\approx_F\langle 1,b\rangle\otimes q_2$. 从而 $q\approx_F(\langle 1,b\rangle\otimes q_2)\otimes\langle 1,a\rangle\approx_F\langle 1,b\rangle\otimes(q_2\otimes\langle 1,a\rangle)$.

(2)$b_1=0$. 此时 $b=ac$. 由定理 5.3.1, $bq_1=a(cq_1)\approx_F aq_1$. 从而 $q=q_1\oplus aq_1\approx_F q_1\oplus bq_1\approx_F\langle 1,b\rangle\otimes q_1$.

(3)b_1 与 c 全不为 0. 此时, $b\in D_F(\langle b_1,ac\rangle)$. 由归纳假定, $q_1\approx_F\langle 1,b_1\rangle\otimes\sigma_1$, 其中 σ_1 是 F 上的一个 $n-2$ 重 Pfister 型. 由情况 (2) 的证明可见, $q\approx_F\langle 1,ac\rangle\otimes q_1$. 从而 $q\approx_F\langle 1,ac\rangle\otimes\langle 1,b_1\rangle\otimes\sigma_1\approx_F\langle 1,b_1,ac,ab_1c\rangle\otimes\sigma_1$. 由命题 5.1.5, 有 $\langle b_1,ac\rangle\approx_F\langle b,bab_1c\rangle$. 于是, $\langle 1,b_1,ac,ab_1c\rangle\approx_F\langle 1,b,bab_1c,ab_1c\rangle\approx_F\langle 1,b\rangle\otimes\langle 1,ab_1c\rangle$. 从而得到 $q\approx_F\langle 1,b\rangle\otimes(\langle 1,ab_1c\rangle\otimes\sigma_1)$.

综上所述, 定理获证.

现在, 我们给出一个将要应用的重要结果, 这个结果与用 Pfister 型表示域中元素的平方和有关.

定理 5.3.3 若域 F 上的每个 n 重 Pfister 型都能表示 F 中任意两个元素的非零平方和, 则对于任意自然数 m, F 上的每个 n 重 Pfister 型能表示 F 中任何 m 个元素的非零平方和.

证明 当 $n=0$ 时, 定理显然成立. 以下设 $n>0$, 并且对 m 使用归纳法.

设 $q=\langle 1\rangle\oplus\varrho$ 是 F 上的一个 n 重 Pfister 型. 对于任意 $c\in\dot{F}$, 由定理的条件有 $c^2=c^2+0^2\in D_F(q)$. 从而定理在 $m=1$ 时成立. 假定定理在 $m=k$ 时成立. 今设 $c=a+b^2$ 且 $c\neq 0$, 其中 a 是 F 中 k 个元素的非零平方和, $b\in\dot{F}$. 我们将证明: $c\in D_F(q)$. 如果 q 是迷向的, 则由命题 5.1.3(2), 立即有 $c\in D_F(q)$. 因此, 不妨设 q 是反迷向的. 由归纳假定 $a\in D_F(q)$. 从而 $a=e^2+d$, 其中 $e\in F$, $d\in D_F(\varrho)\cup\{0\}$. 当 $d=0$ 时, 由定理的条件, 即有 $c=e^2+b^2\in D_F(q)$. 今设 $d\neq 0$. 此时, 由定理 5.3.2, $q\approx_F\langle 1,d\rangle\otimes q_1$, 其中 q_1 是 F 上一个 $n-1$ 重 Pfister 型. 这样, 我们有

$$\begin{aligned}q\oplus -cq &\approx_F\langle 1,-c\rangle\otimes q\approx_F\langle 1,-c\rangle\otimes\langle 1,d\rangle\otimes q_1\\&\approx_F\langle 1,-c,d,-cd\rangle\otimes q_1\\&\approx_F(\langle -c,d\rangle\otimes q_1)\oplus(\langle 1,-cd\rangle\otimes q_1).\end{aligned}$$

令 $q_1=\langle 1\rangle\oplus\varrho_1$, 则有

$$q \oplus -cq \approx_F \langle -c, d\rangle \oplus \langle -c, d\rangle \otimes \varrho_1 \oplus \langle 1, -cd\rangle \otimes q_1.$$

由定理的条件, $e^2+b^2 \in D_F(\langle 1,-cd\rangle \otimes q_1) \cup \{0\}$. 从而有 $u \in F^{2^n}$, 使得 $e^2+b^2 = (\langle 1,-cd\rangle \otimes q_1)(u)$. 记 $\sigma := \langle -c,d\rangle \oplus \langle -c,d\rangle \otimes \varrho_1 \oplus \langle 1,-cd\rangle \otimes q_1$, 而 $\theta = (0,0,\cdots,0)$ 是向量空间 F^{2^n-2} 中的零向量. 于是, 对于 $F^{2^{n+1}}$ 中非零向量 $\xi = (1,1,\theta,u)$, 有 $\sigma(\xi) = -c+d+e^2+b^2 = 0$. 因而 σ 是迷向的, 从而 $q \oplus -cq$ 也是迷向的. 于是有非零向量 $(\alpha,\beta) \in F^{2^n} \times F^{2^n}$, 使得 $q(\alpha) - cq(\beta) = 0$, 即 $cq(\beta) = q(\alpha)$. 若 $q(\beta) = 0$, 则 $q(\alpha) = 0$. 由于 q 是反迷向的, 从而 $\alpha = \beta = 0$, 但这与 $(\alpha,\beta) \neq 0$ 矛盾. 因此 $q(\beta) \neq 0$. 再由定理 5.3.1 的推论, $c = q(\alpha)q(\beta)^{-1} \in D_F(q)$. 至此定理获证.

现在, 我们通过上面关于 Pfister 型的结果, 针对非实域研究 -1 的平方和表示中所需的平方项个数.

定义 5.3.2 设 F 是一个域. 若 -1 不能表为 F 中元素的平方和, 则记 $\ell(F) = \infty$; 若 -1 能表为 F 中元素的平方和, 则规定 $\ell(F)$ 是 -1 的平方和表示中平方项的最小个数. 同时, 称 $\ell(F)$ 为域 F 的层.

显然, 域 F 是一个实域, 当且仅当 $\ell(F) = \infty$. 此外, 对于域 F 的任意一个扩张 K, 有 $\ell(K) \leqslant \ell(F)$. 为书写方便起见, 对于任意自然数 n 以及域 F 上任意型 ϱ, 规定: $n \times \varrho = \overbrace{\varrho \oplus \cdots \oplus \varrho}^{n\text{重}}$.

定理 5.3.4(Pfister) 对于任意域 F, $\ell(F) = \infty$ 或者 $\ell(F) = 2^m$, 其中 m 是一个非负整数.

证明 不妨设 $\ell(F) = s$, 其中 s 是一个正整数. 选取非负整数 m, 使得 $2^m \leqslant s < 2^{m+1}$. 令 $q = 2^{m+1} \times \langle 1\rangle$ 为 F 上 2^{m+1} 重 Pfister 型, 则有

$$q = \langle 1\rangle \oplus (2^{m+1}-1) \times \langle 1\rangle.$$

注意到, $s \leqslant 2^{m+1}-1$. 从而由条件知, $-1 \in D_F(s \times \langle 1\rangle) \subseteq D_F((2^{m+1}-1)\times\langle 1\rangle)$. 由定理 5.3.2 知, $q \approx_F \langle 1,-1\rangle \otimes q_1$, 其中 q_1 是 F 上一个 2^m 重 Pfister 型. 令 $q_1 = \langle a_1,\cdots,a_{2^m}\rangle$, 则 $q \approx_F \langle a_1,-a_1\rangle \oplus \cdots \oplus \langle a_{2^m},-a_{2^m}\rangle$. 再根据命题 5.1.3 的推论, 有

$$q \approx_F 2^m \times \langle 1\rangle \oplus 2^m \times \langle -1\rangle.$$

由 Witt 消去定理有

$$2^m \times \langle 1\rangle = 2^m \times \langle -1\rangle.$$

根据命题 5.1.2, $-1 \in D_F(2^m \times \langle 1\rangle)$. 由 $\ell(F)$ 的定义可知, $s = 2^m$. 证毕.

§5.4 Pfister 定理

在本节中，我们将建立重要的 Pfister 定理，这个定理是 A. Pfister 在 1967 年得到的. 对于实闭域上所有半正定多项式的平方和表示， Pfister 定理给出了它们的平方项个数的一个上界. 为建立 Pfister 定理，我们还需要域论中一个重要的定理，这个定理是由我国代数学家曾炯之 (C. C. Tsen) 在 1936 年首次获得的. 其后， S. Lang 在 1951 年再次发现这一结果. 为证明这个定理，我们先给出一些预备 知识.

首先，我们需要代数几何中最基本的一条定理 ——Hilbert 零点定理，这条定理已有一百多年的历史.

命题 5.4.1(Hilbert 零点定理) 设 F 是任意域， Ω 是它的代数闭包， $f_1, \cdots, f_r, g \in F[x_1, \cdots, x_n]$. 若对于任何 $(a_1, \cdots, a_n) \in \Omega^n$, 只要 $f_i(a_1, \cdots, a_n) = \cdots = f_r(a_1, \cdots, a_n) = 0$, 总有 $g(a_1, \cdots, a_n) = 0$, 则对于某个自然数 k, 有 $g^k \in Id(f_1, \cdots, f_r)$, 此处 $Id(f_1, \cdots, f_r)$ 是多项式环 $F[x_1, \cdots, x_n]$ 中由 $f_1, \cdots, f_r$ 生成的理想.

引理 5.4.2 设 F 是一个代数闭域， $f_1, \cdots, f_r$ 是多项式环 $F[x_1, \cdots, x_n]$ 中的齐次多项式. 若 $n > r$, 则方程组 $f_1 = \cdots = f_r = 0$ 在 F 中有非零解，即异于 $(0, \cdots, 0)$ 的解.

证明 用反证法. 假设方程组 $f_1 = \cdots = f_r = 0$ 只有零解 $(0, \cdots, 0)$. 由命题 5.4.1, 对于每个 $i = 1, \cdots, n$, 存在一个自然数 k_i, 使得有 $x_i^{k_i} \in Id(f_1, \cdots, f_r)$. 取 $k = \max\{k_i \mid i = 1, \cdots, n\}$, 显然有 $x_i^k \in Id(f_1, \cdots, f_r)$, $i = 1, \cdots, n$. 从而有

$$x_i^k = g_{i1}f_1 + \cdots + g_{ir}f_r, \quad i = 1, \cdots, n, \tag{$\star$}$$

其中 $g_{ij} \in F[x_1, \cdots, x_n]$, $i = 1, \cdots, n$; $j = 1, \cdots, r$.

比较上式两边的 k 次部分, 从而可假定诸多项式 g_{ij} 都是齐次的. 于是当 $g_{ij} \neq 0$ 时，其次数 $\deg g_{ij} < k$.

据此，可以断言：每个单项式都可以在域 $K := F(f_1, \cdots, f_r)$ 上由次数不超过 $n(k-1)+1$ 的项 (即系数为 1 的单项式) 线性表示. 事实上，对于每个 n 元单项式 M, $M = cM_1$, 其中 c 为 M 的系数， M_1 是系数为 1 的单项式. 从而，我们可以选取如下的表达式

$$M = h_1G_1 + \cdots + h_sG_s, \tag{$\star\star$}$$

其中 $h_j \in K$, G_j 是系数为 1 的单项式， $j = 1, \cdots, s$, 同时使得上式中每个 G_j 的次数都尽可能小. 此时可断定 $\deg G_j < n(k-1)+1$, $j = 1, \cdots, s$. 事实上，如若不然，则不妨设 $\deg G_1 \geqslant n(k-1)+1$. 于是对某个 $m \in \{1, \cdots, n\}$, 有 $G_1 = x_m^k G_0$,

其中 G_0 是一个系数为 1 的单项式. 从而由等式 $(\star)$ 和 $(\star\star)$ 有

$$\begin{aligned} M &= h_1(g_{m1}f_1 + \cdots + g_{mr}f_r)G_0 + h_2G_2 + \cdots + h_sG_s \\ &= (f_1h_1)(g_{m1}G_0) + \cdots + (f_rh_1)(g_{mr}G_0) + h_2G_2 + \cdots + h_rG_r, \end{aligned}$$

其中 $f_jh_1 \in K$, $j = 1, \cdots, r$. 此时, $\deg(g_{mj}G_0) < \deg G_1$, $j = 1, \cdots, r$. 展开诸 $g_{mj}G_0$, 我们将得到一个形如 $(\star\star)$ 的表达式, 其中单项式的次数更低, 这与等式 $(\star\star)$ 的取法相矛盾.

这样, $K[x_1, \cdots, x_n]$ 作为 K 上的向量空间是有限维的. 从而 $x_1, \cdots, x_n$ 都是 K 上的代数元. 注意到 $F(x_1, \cdots, x_n) = K(x_1, \cdots, x_n)$, 从而, $F(x_1, \cdots, x_n)$ 关于 F 的超越次数和 K 关于 F 的超越次数相等. 显然, K 关于 F 的超越次数不超过 r. 从而, $F(x_1, \cdots, x_n)$ 关于 F 的超越次数不超过 r 矛盾. 引理获证.

现在, 我们给出下面的定义.

定义 5.4.1　设 i 是个非负实数. 一个域 F 称为一个 C_i- 域, 如果对于任何自然数 d, 每个 F 上次数为 d, 而未定元个数多于 d^i 的齐次多项式在 F 中有非零的零点.

由引理 5.4.2 知, 任何代数闭域都是 C_0- 域. 实际上, 我们有如下的命题.

命题 5.4.3　一个域 F 为 C_0- 域, 当且仅当 F 是代数闭域.

证明　只须证明必要性. 设 F 是一个 C_0- 域, 且 $f(x) = x^d + a_1x^{d-1} + \cdots + a_d$ 为 F 上任意多项式, 其中 $d \geqslant 1$. 由于 $2 > 1 = d^0$, 从而齐次多项式 $g(x, y) = x^d + a_1x^{d-1}y + \cdots + a_dy^d$ 在 F 中有非零的零点 (b, c). 此时应有 $c \neq 0$ (否则, 有 $b = 0$). 从而 $f(x) = 0$ 在 F 中有解 bc^{-1}. 这表明域 F 是代数闭域. 证毕.

定义 5.4.2　设 i 是一个非负整数. 域 F 上一个次数 d 大于 1 的齐次多项式称作是 F 上的一个 i 级范式, 如果它含有 d^i 个未定元, 而且这个齐次式只有浅显零点 $(0, \cdots, 0)$.

设 F 是任意域, 则对于任意自然数 $d > 1$, x^d 都是 F 上的 0 级范式.

引理 5.4.4　设域 F 上有一个 i 级范式, 则域 $F(t)$ 上有一个 $i+1$ 级范式, 这里 t 是 F 上的未定元.

证明　设 $N(x_1, \cdots, x_{d^i})$ 是 F 上一个次数为 d 的 i 级范式. 现证明: 下面的多项式

$$N_1 = N(x_1, \cdots, x_{d^i}) + N(x_{d^i+1}, \cdots, x_{2d^i})t + \cdots + N(x_{(d-1)d^i+1}, \cdots, x_{d^{i+1}})t^{d-1}$$

是 $F(t)$ 上的一个 $i+1$ 级范式.

首先, N_1 是次数为 d, 且含 d^{i+1} 个未定元的 $F(t)$ 上齐次式. 其次, 假若 N_1 在 $F(t)$ 中有一个非浅显零点 $(u_1, \cdots, u_{d^{i+1}})$. 由于 N_1 是齐次的, 从而可进一步假定 $u_j \in F[t]$, $j = 1, \cdots, d^{i+1}$, 且并非每个 u_j 都能被 t 整除. 令 k 是 $1, \cdots, d^{i+1}$ 中

最小足标，使得 u_k 不能被 t 整除，且设 $sd^i+1\leqslant k\leqslant(s+1)d^i$, 其中 $0\leqslant s\leqslant d-1$. 由于 N 是 d 次齐次式，且 t 整除 u_j, $j=1,\cdots,sd^i$, 从而有

$$N(u_1,\cdots,u_{d^i})+\cdots+N(u_{(s-1)d^i+1},\cdots,u_{sd^i})t^{s-1}\equiv 0\ (\operatorname{mod} t^d).$$

此外，显然有

$$N(u_{(s+1)d^i+1},\cdots,u_{(s+2)d^i})t^{s+1}+\cdots+N(u_{(d-1)d^i+1},\cdots,u_{d^{i+1}})t^{d-1}\equiv 0\ (\operatorname{mod} t^{s+1}).$$

由于 $N_1(u_1,\cdots,u_{d^{i+1}})=0$ 且 $d\geqslant s+1$, 从而有

$$N(u_{sd^i+1},\cdots,u_{(s+1)d^i})t^s\equiv 0\ (\operatorname{mod} t^{s+1}).$$

于是有

$$N(u_{sd^i+1},\cdots,u_{(s+1)d^i})\equiv 0\ (\operatorname{mod} t).$$

因而有 $N(a_{sd^i+1},\cdots,a_{(s+1)d^i})=0$, 其中 $a_j=u_j(0)\in F$, $j=sd^i+1,\cdots,(s+1)d^i$. 注意到 $a_k=u_k(0)\neq 0$, 从而范式 N 在 F 中有非浅显零点，矛盾. 因此，N_1 是 $F(t)$ 上的一个 $i+1$ 级范式. 证毕.

若 $N(x_1,\cdots,x_{d^i})$ 是域 F 上的一个次数为 d 的 i 级范式，则容易验证

$$N(N(x_1,\cdots,x_{d^i}),N(x_{d^i+1},\cdots,x_{2d^i}),\cdots,N(x_{d^{2i}-d^i+1},\cdots,x_{d^{2i}}))$$

是 F 上一个次数为 d^2 的 i 级范式. 由于 $d>1$, 从而 $d^2>d$. 如此进行下去，我们可得到 F 上一个具有充分大次数的 i 级范式. 此一事实将在下面得到重要应用.

引理 5.4.5 设 F 是一个 C_i- 域，且 F 上有一个 i 级范式. 又设 $f_1,\cdots,f_r$ 是 F 上 r 个次数为 d 且含未定元 $x_1,\cdots,x_n$ 的齐次多项式. 若 $n>rd^i$, 则方程组 $f_1=\cdots=f_r=0$ 在 F 中有非零解.

证明 先考虑 $i=0$ 的情形. 由命题 5.4.3 知，F 是代数闭域. 由条件有 $n>rd^0=r$. 从而由引理 5.4.2 即得结论. 以下设 $i>0$.

注意到 $n-rd^i>0$. 由前面的事实，F 上有一个次数充分大的 i 级范式 N, 其次数 e 满足 $e^i>\dfrac{r^2d^i}{n-rd^i}+r$. 再设 $e^i=rs+t$, $0\leqslant t<r$. 于是有 $rs+r>rs+t=e^i>\dfrac{r^2d^i}{n-rd^i}+r$, 即有 $s>\dfrac{rd^i}{n-rd^i}$. 从而可得 $ns>rsd^i+rd^i>rsd^i+td^i=e^id^i=(ed)^i$.

由于 N 中未定元个数 e^i 满足 $e^i=rs+t\geqslant rs$, 从而可构造 F 上的如下齐次式

$$\begin{aligned}H=N(&f_1,\cdots,f_r,f_1(x_{n+1},\cdots,x_{2n}),\cdots,f_r(x_{n+1},\cdots,x_{2n}),\cdots,\\&f_1(x_{(s-1)n+1},\cdots,x_{sn}),\cdots,f_r(x_{(s-1)n+1},\cdots,x_{sn}),0,\cdots,0).\end{aligned}$$

显然，H 的次数是 ed, 且含有 ns 个未定元. 由于 F 是一个 C_i- 域，且 $ns>(ed)^i$,

从而 H 在 F 中有一个非浅显零点 $(a_1,\cdots,a_{sn})$. 因为 N 是一个范式，从而有

$$f_j(a_{(k-1)n+1},\cdots,a_{kn})=0,\ j=1,\cdots,r;\ k=1,\cdots,s.$$

这表明：方程组 $f_1=\cdots=f_r=0$ 在 F 中有解 $(a_{(k-1)n+1},\cdots,a_{kn})$, $k=1,\cdots,s$. 显然，这些解中至少有一个是非零解. 证毕.

引理 5.4.6 设 F 是一个 C_i- 域，且 F 上有一个 i 级范式，则 $F(t)$ 是一个 C_{i+1}- 域，其中 t 是 F 上的未定元.

证明 设 $f(x_1,\cdots,x_n)$ 是域 $F(t)$ 上的一个次数为 d 的齐次多项式，其中 $n>d^{i+1}$. 我们要证明，齐次方程 $f=0$ 在 $F(t)$ 中有非零解.

不失一般性，可以假定 f 的系数都是 F 上含 t 的多项式，且令 r 是 f 关于 t 的次数. 由于 $\lim\limits_{s\to\infty}\dfrac{sd+r+1}{s+1}=d<\dfrac{n}{d^i}$, 从而有充分大的自然数 s, 使得 $\dfrac{sd+r+1}{s+1}<\dfrac{n}{d^i}$. 此时有 $n(s+1)>(sd+r+1)d^i$. 令 $x_j=x_{j0}+x_{j1}t+\cdots+x_{js}t^s$, $j=1,\cdots,n$. 其中 $x_{jk}(1\leqslant j\leqslant n,\ 0\leqslant k\leqslant s)$ 是 $n(s+1)$ 个互不相同的未定元. 从而有

$$f(x_1,\cdots,x_n)=f_0+f_1t+\cdots+f_{sd+r}t^{sd+r},$$

其中 $f_0,\cdots,f_{sd+r}$ 是 F 上含 $n(s+1)$ 个未定元 x_{jk} 且次数为 d 的齐次多项式.

由引理 5.4.5 知，$f_0,\cdots,f_{sd+r}$ 在 F 中有一个非零的公共零点

$$(a_{10},\cdots,a_{1s},\cdots,a_{n0},\cdots,a_{ns}).$$

于是 $f=0$ 在 $F(t)$ 中有非零解 $(u_1,\cdots,u_n)$, 其中 $u_j=a_{j0}+a_{j1}t+\cdots+a_{js}t^s$, $j=1,\cdots,n$. 证毕.

现在，可以证明下面的重要结果.

定理 5.4.7(曾炯之 -Lang) 设 F 是个代数闭域，$x_1,\cdots,x_n$ 是 F 上的未定元，则 $F(x_1,\cdots,x_n)$ 是一个 C_n- 域，并且它有一个 n 级范式.

证明 对 n 用归纳法. 由命题 5.4.3 以及前面的讨论，F 是一个 C_0- 域，而且 F 有一个 0 级范式. 故定理在 $n=0$ 时成立. 今设 $n\geqslant 1$, 且定理对 $n-1$ 成立. 由引理 5.4.6 和 5.4.4 知，$F(x_1,\cdots,x_{n-1},x_n)$ 是一个 C_n- 域，并且它有一个 n 级范式. 证毕.

由上面的曾炯之 -Lang 定理，我们立即可以得到一个有用的结果.

推论 设 F 是代数闭域，则 $F(x_1,\cdots,x_n)$ 上每个维数大于 2^n 的正则型都是迷向的.

现在，我们可以用上面推论来证明 Pfister 所得到的如下结果.

定理 5.4.8(Pfister) 设 R 是个实闭域，则有理函数域 $R(x_1,\cdots,x_n)$ 中任意多个元素的平方和都可表为 2^n 个元素的平方和.

证明 记 $F := R(x_1, \cdots, x_n)$. 由定理 5.2.3, 只须证明 F 上每个 n 重 Pfister 型能够表示 F 中任意两个元素的非零平方和. 从而 n 重 Pfister 型 $2^n \times \langle 1 \rangle$ 可表示 F 中任意多个元素的非零平方和. 这样, 定理获得证明.

设 q 是 F 上的一个 n 重 Pfister 型, 且 $b = b_1^2 + b_2^2 \neq 0$, 其中 $b_1, b_n \in F$. 不失一般性, 可设 $b_2 \neq 0$. 若 q 在 F 上是迷向的, 则由命题 5.1.3(2), $b \in D_F(q)$. 以下设 q 在 F 上是反迷向的. 令 $\Omega = R(\sqrt{-1})$, 则 Ω 是代数闭域. 再令 $K = \Omega(x_1, \cdots, x_n)$. 易知 $K = F(\eta)$, 其中 $\eta = b_1 + b_2\sqrt{-1}$.

下面将证明 q 在 K 上是泛的, 即 $D_K(q) = \dot{K}$. 由命题 5.1.3(2), 可以设 q 在 K 上是反迷向的. 设 $d \in \dot{K}$. 由上面的推论, 型 $q \oplus \langle -d \rangle$ 在 K 上是迷向的. 从而, 对某个非零向量 $(\alpha, a) \in K^{2^n} \times K$, 有 $q(\alpha) - da^2 = 0$. 若 $a = 0$, 则 α 必为 K^{2^n} 中的非零向量, 且 $q(\alpha) = 0$. 从而 q 在 K 上是迷向的, 矛盾. 因此 $a \neq 0$, 从而 $d = a^{-2}q(\alpha) = q(a^{-1}\alpha) \in D_K(q)$. 这表明 q 在 K 上是泛的.

于是, 对于某个非零向量 $\beta \in K^{2^n}$, $\eta = q(\beta)$. 记 $q(\bar{x}, \bar{y})$ 为型 q 所对应的双线性函数, 即对于任意 $\bar{x}, \bar{y} \in K^{2^n}$, $q(\bar{x}, \bar{y}) = \dfrac{1}{4}[q(\bar{x}+\bar{y}) - q(\bar{x}-\bar{y})]$. 又记 $\beta = u + \eta v$, 其中 $u, v \in F^{2^n}$. 从而有 $\eta = q(u+\eta v) = q(u) + 2\eta q(u, v) + \eta^2 q(v)$. 注意到 $\eta^2 - 2b_1\eta + b = 0$. 于是 $\eta = [q(u) - bq(v)] + 2[q(u, v) + b_1 q(v)]\eta$. 由于 $1, \eta$ 在域 F 上是线性无关的, 从而 $q(u) - bq(v) = 0$, 即 $q(u) = bq(v)$. 若 $q(v) = 0$, 则 $q(u) = 0$. 又因 q 在 F 上是反迷向的, 从而 $u = v = 0$. 于是 $\beta = 0$, 矛盾. 因此 $q(v) \neq 0$. 再由定理 5.3.1 的推论, 有 $b \in D_F(q)$. 至此, 定理告证.

结合定理 4.1.3 的推论 2 和定理 5.4.8, 立即得到以下定理.

定理 5.4.9 对于任何实闭域 R, R 上每个半正定 n 元多项式 $f(x_1, \cdots, x_n)$ 都可表示为 $R(x_1, \cdots, x_n)$ 中 2^n 个元素的平方和.

必须指出, 定理 5.4.9 仅仅给出实闭域上半正定 n 元多项式的平方和表示中项数的一个上界. 对于任意自然数 n, 至今还不能给出一个表达式来描述更精确的上界.

§5.5 半　序

在本节中, 我们将引进域上一个与二次型相关的序关系 —— 半序. 域上的半序可看作域的序的一个推广, 它们满足第一章中序所适合的许多结论.

定义 5.5.1 域 F 上一个二元关系 $\leqslant$ 称作 F 的一个半序, 如果它满足定义 1.1.3 中条件 (1~5), 同时满足条件 (6′): $0 < 1$, 且对于任意 $a, b \in F$, 只要 $0 \leqslant a$, 总有 $0 \leqslant ab^2$.

类似序与正锥之间的关系, 相应地可给出下面的定义.

定义 5.5.2 域 F 的一个子集 P 称作半锥, 若下列条件成立:

(1) $P+P\subseteq P$;

(2) $1\in P$ 且 $F^2\cdot P\subseteq P$;

(3) $P\cap -P=\{0\}$;

(4) $F=P\cup -P$.

显然，若 $\leqslant$ 是域 F 的一个半序，则 $\leqslant$ 惟一地对应于 F 的半锥 $P_{\leqslant}=\{a\in F\mid 0\leqslant a\}$; 反过来，对于域 F 的半锥 P, P 惟一地对应 F 的一个半序 $\leqslant_P$, 使得 $a\leqslant_P b$, 当且仅当 $b-a\in P$. 同样，如下事实成立：若 P_1 和 P_2 均为域 F 的半锥，且 $P_1\subseteq P_2$, 则 $P_1=P_2$.

域上的序显然是半序，但半序未必为序. 域的一个半序称作真半序，如果它不是一个序. 在后面，将给出一个真半序的例子.

与亚正锥相对应，可给出下面定义.

定义 5.5.3　域 F 的一个非空子集 T 称作亚半锥，如果下列条件成立：

(1) $T+T\subseteq T$;

(2) $F^2\cdot T\subseteq T$;

(3) $T\cap -T=\{0\}$.

显然，每个半锥都是亚半锥. 同时，上面的条件 (2) 等价于：$S_F\cdot T\subseteq T$, 这里 S_F 为 F 的弱亚正锥. 此外，$\{0\}$ 是任意域的亚半锥. 注意这样一个事实：若域 F 有一个非零的亚半锥，则 F 必为实域. 事实上，如若不然，则 $-T\subseteq S_F\cdot T\subseteq T$, 这矛盾于定义 5.5.3 中条件 (3).

引理 5.5.1　设 T 是实域 F 的一个亚半锥. 若 $a\in F$, 但 $-a\notin T$, 则 $T+aS_F=\{t+as\mid t\in T,\, s\in S_F\}$ 为 F 的一个包含 a 的亚半锥.

证明　显然，$T\subseteq T+aS_F$, 且 $T+aS_F$ 满足定义 5.5.3 中条件 (1) 和 (2). 设 $b\in (T+aS_F)\cap -(T+aS_F)$, 则 $b=t_1+as_1=-(t_2+as_2)$, 其中 $t_1,\, t_2\in T$, 且 $s_1,\, s_2\in S_F$. 从而有 $t_1+t_2=-a(s_1+s_2)$. 如若 $s_1+s_2\neq 0$, 则 $(s_1+s_2)^{-1}\in S_F$. 由此可推出矛盾：$-a=(s_1+s_2)^{-1}(t_1+t_2)\in S_F\cdot T\subseteq T$. 于是，$s_1+s_2=0$. 由于 F 是实域，从而 $s_1=s_2=0$. 此时，$t_1=-t_2\in T\cap -T=\{0\}$, 即 $t_1=t_2=0$. 因而，$b=0$. 由定义 5.5.3 知，上面引理获证.

借助于上面引理，通过类似于定理 1.1.2 的证明方法，可获得如下定理.

定理 5.5.2　设 T 是域 F 的一个亚半锥，使得 $1\in T$, 且记 $\mathcal{Y}_F$ 为域 F 的所有包含 T 的半锥组成的集合，则

$$T=\bigcap_{P\in\mathcal{Y}_F}P.$$

推论 1　设 F 是一个实域，则 S_F 为域 F 的所有半锥的交集.

推论 2　域 F 为实域，当且仅当 F 有一个半序 (半锥).

推论 3　若域 F 仅有惟一序 (或半序), 则 F 没有真半序.

由于半序所满足的条件弱于序，从而序所满足的某些事实对于半序却可能不成立．然而，我们可建立下面结果.

命题 5.5.3　设 $\leqslant$ 是域 F 的一个半序, 则对于任意的 $a, b \in F$, 下列事实 成立：

(1) 若 $0 < a$, 则 $0 < a^{-1}$;

(2) 若 $0 < a < b$, 则 $a^2b < ab^2$, 且 $b^{-1} < a^{-1}$;

(3) 若 $1 < b$, 则 $b < b^2$;

(4) 若 $0 < a < 1$, 则 $a^2 < a$;

(5) 若 $0 < a < b$ 且 $a \in S_F$, 则 $a^2 < b^2$;

(6) 若 $0 < a < b$ 且 $b \in S_F$, 则 $a^2 < b^2$;

(7)$\leqslant$ 是 F 的一个序，当且仅当由关系式 $0 < a < b$, 可推出 $a^2 < b^2$.

证明　(1) 由定义 5.5.1 中条件 (6′) 有，$(a^{-1})^2 \cdot 0 < (a^{-1})^2 \cdot a$, 即 $0 < a^{-1}$.

(2) 由事实 (1) 知，$0 < a^{-1}$ 且 $0 < (b-a)^{-1}$. 由此有 $0 < a^{-1} + (b-a)^{-1}$. 再由事实 (1) 有 $0 < (a^{-1} + (b-a)^{-1})^{-1}b^2$, 即 $0 < ab^2 - a^2b$. 从而 $a^2b < ab^2$. 此时有 $(a^2b)(a^{-1}b^{-1})^2 < (ab^2)(a^{-1}b^{-1})^2$, 即 $b^{-1} < a^{-1}$.

(3) 在事实 (2) 中取 $a = 1$ 即可.

(4) 在事实 (2) 中取 $b = 1$ 即可.

(5) 由事实 (2) 知，$a^2b < ab^2$. 注意到 $a^{-1} \in S_F$, 从而 $ab < b^2$. 又由于 $a < b$ 且 $a \in S_F$, 从而 $a^2 < ab$. 因而，$a^2 < b^2$.

(6) 类似于 (5) 可证.

(7) 必要性显然．现设 $0 < a$ 且 $0 < b$, 其中 $a, b \in F$. 若 $a = b$, 则 $ab = a^2 > 0$. 下设 $a < b$, 则有 $0 < b - a < a + b$. 由所设知，$(b-a)^2 < (a-b)^2$. 由此可得，$0 < 4ab$. 因此，总有 $0 < ab$. 这表明：$\leqslant$ 是 F 的一个序．证毕.

设 P 是域 F 的一个半锥，K 是域 F 的一个扩张．K 的一个半锥 Q 称作 P 在 K 上的一个拓展，若 $Q \cap F = P$. 关于半锥 (半序) 在域扩张上的可拓展性，我们可建立如下命题.

命题 5.5.4　设 K 是域 F 的一个扩张，P 是 F 的一个半锥，则 P 可拓展为 K 的一个半锥，当且仅当对于任意有限个非零 $a_1, \cdots, a_n \in P$, 型 $\langle a_1, \cdots, a_n \rangle$ 在 K 上是反迷向的.

证明　必要性显然．为证明充分性，构造 K 的如下子集:

$$S_K(P) = \left\{ \sum_{i=1}^{n} a_i \alpha_i^2 \mid n\text{为自然数}, a_1, \cdots, a_n \in P, \alpha_1, \cdots, \alpha_n \in K \right\}.$$

显然，$1 \in S_K(P)$. 进一步可验证：$S_K(P)$ 为域 K 的一个亚半锥．由定理 5.5.2 知，K 有一个半锥 Q, 使得 $S_K(P) \subseteq Q$. 此时易知 $Q \cap F = P$. 证毕.

根据命题 5.5.4 以及 Springer 定理 (定理 5.1.4), 可建立类似于定理 1.3.4 的两个推论的如下结果.

定理 5.5.5 设 P 是域 F 的一个半锥, 则对于 F 的如下扩张 K, P 可拓展为 K 的一个半锥:

(1) $[K:F]$ 为奇数;

(2) $K=F(\sqrt{a})$, 其中 $a\in F$, 使得 $aP\subseteq P$, 且 $\sqrt{a}$ 是多项式 x^2-a 在 F 的代数闭包中的一个根.

证明 (1) 对于任意有限个非零元 $a_1,\cdots,a_n\in P$, 型 $\langle a_1,\cdots,a_n\rangle$ 在 F 上是反迷向的. 由定理 5.1.4 知, $\langle a_1,\cdots,a_n\rangle$ 在 K 上也是反迷向的. 由命题 5.5.4 知, P 可拓展为 K 的一个半锥.

(2) 不失一般性, 可假定 $\sqrt{a}\notin F$. 设 $a_1,\cdots,a_n\in P$, 且它们都不为零, 则型 $\langle a_1,\cdots,a_n\rangle$ 在 F 上是反迷向的. 如果

$$a_1(b_1+c_1\sqrt{a})^2+\cdots+a_n(b_n+c_n\sqrt{a})^2=0,$$

其中 $b_i,c_i\in F$, $i=1,\cdots,n$, 那么

$$\sum_{i=1}^n a_i(b_i^2+ac_i^2)+2\left(\sum_{i=1}^n a_ib_ic_i\right)\sqrt{a}=0.$$

由此有 $\sum_{i=1}^n a_i(b_i^2+ac_i^2)=0$. 于是 $\sum_{i=1}^n a_ib_i^2=-a\sum_{i=1}^n a_ic_i^2\in P\cap -P=\{0\}$, 即有 $\sum_{i=1}^n a_ib_i^2=\sum_{i=1}^n a_ic_i^2=0$. 由于 $\langle a_1,\cdots,a_n\rangle$ 在 F 上是反迷向的, 从而 $b_i=c_i=0$, $i=1,\cdots,n$. 因而 $b_i+c_i\sqrt{a}=0$, $i=1,\cdots,n$. 这表明: $\langle a_1,\cdots,a_n\rangle$ 在 $K=F(\sqrt{a})$ 上是反迷向的. 由命题 5.5.4 知, P 可拓展为 K 的一个半锥. 证毕.

在 §1.4 中, 我们讨论了序的阿基米德性与非阿基米德性. 类似地, 可给出下列定义.

定义 5.5.4 设 $\leqslant$ 是域 K 的一个半序, F 是 K 的一个子域. 称 $\leqslant$ 是在 F 上的阿基米德半序, 若对于每个 $\alpha\in K$, 有 $a\in F$, 使得 $-a\leqslant\alpha\leqslant a$. 特别地, 在有理数子域 $\mathbb{Q}$ 上的阿基米德半序简称阿基米德半序.

下面定理表明, 阿基米德半序与阿基米德序是同一事物.

定理 5.5.6 域 F 的每个阿基米德半序必是一个序.

证明 设 $\leqslant$ 是域 F 的一个阿基米德半序, $0<a$ 且 $0<b$, 其中 $a,b\in F$. 不妨设 $a\leqslant b$, 则有 $0\leqslant b-a<b+a$. 注意到, 由同样的证明可推得, 命题 1.4.3 对于半序也是成立的. 从而有 $r\in\mathbb{Q}$, 使得 $0\leqslant b-a<r<b+a$. 由于 $r\in S_F$, 从而由命题 5.5.3 中结论 (5) 和 (6) 有, $(b-a)^2<r^2<(b+a)^2$. 由此有 $0<4ab$, 即 $0<ab$.

因此，$\leqslant$ 是一个序．证毕．

根据定理 5.5.6 可知，有理数域 $\mathbb{Q}$ 没有真半序．实际上，可证明：有理数域 $\mathbb{Q}$ 的任意代数扩张也没有真半序．为此，我们需要如下结果 (参见引理 1.2.2).

定理 5.5.7 设 K 是域 F 的一个代数扩张，则对于任意 $\alpha \in K$, 有 $M \in S_F$, 使得对于 K 的每个半序 $\leqslant$, 都有 $-M < \alpha < M$.

证明 设 α 在 F 上的极小多项式为

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n,$$

其中 $a_1, \cdots, a_n \in F$.

令 $M = \frac{1}{2}(n + 1 + a_1^2 + \cdots + a_n^2) \in S_F$. 设 $\leqslant$ 是 K 的任意一个半序．注意到这样一个基本事实：对于任意 $y, z \in F$, $yz \leqslant \frac{1}{2}(y^2 + z^2)$. 从而当 $\alpha^2 < 1$ 时, $\alpha \leqslant \frac{1+\alpha^2}{2} < 1 < M$, 且 $-\alpha \leqslant \frac{1+(-\alpha)^2}{2} < 1 < M$. 于是，$-M < \alpha < M$. 下设 $\alpha^2 \geqslant 1$, 则 $1 \geqslant \alpha^{-2}$. 从而可知，对于每个自然数 m, $1 \geqslant \alpha^{-2m}$.

由于 $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$, 从而有 $\alpha = -a_1 - a_2\alpha^{-1} - a_n\alpha^{1-n} \leqslant \frac{1}{2}(a_1^2 + 1 + a_2^2 + \alpha^{-2} + \cdots + a_n^2 + \alpha^{2-2n}) \leqslant \frac{1}{2}(n + a_1^2 + \cdots + a_n^2) < M$. 同理可证，$-\alpha < M$, 即 $-M < \alpha$. 证毕．

推论 1 设 $\leqslant$ 是域 F 的一个半序，E 是 F 的一个子域，K 是 F 的一个扩张，且 $\leqslant_K$ 是半序 $\leqslant$ 在 K 上的一个拓展．若 K 是 F 的代数扩张，则 $\leqslant$ 在 E 上是阿基米德的，当且仅当 $\leqslant_K$ 在 E 上是阿基米德的．

推论 2 有理数域 $\mathbb{Q}$ 的任意代数扩张的每个半序都是阿基米德序．

证明 设 K 是 $\mathbb{Q}$ 的任意一个代数扩张，且 $\leqslant$ 是 K 的一个半序．由上面推论 1 知，$\leqslant$ 在 $\mathbb{Q}$ 上是阿基米德的，即 $\leqslant$ 是阿基米德半序．由定理 5.5.6 知，$\leqslant$ 是一个阿基米德序．证毕．

现在，我们来研究二次型与半序之间的联系．首先，将 “符号差” 这一概念与域的半锥联系起来．设 P 是域 F 的一个半锥，$q = \langle a_1, \cdots, a_n \rangle$ 是 F 上一个 n 维型．在 $a_1, \cdots, a_n$ 中，属于 P 的非零元个数与属于 $-P$ 的非零元个数之差称作 q 关于半锥 P 的符号差，且记作 $\mathrm{sgn}_P(q)$ 或 $\mathrm{sgn}_P(\langle a_1, \cdots, a_n \rangle)$.

定理 5.5.8 若 $q = \langle a_1, \cdots, a_n \rangle$ 和 $\varrho = \langle b_1, \cdots, b_n \rangle$ 均为域 F 上的型, 且 $q \approx_F \varrho$, 则对于 F 的每个半锥 P, $\mathrm{sgn}_P(q) = \mathrm{sgn}_P(\varrho)$.

证明 设 $a_1, \cdots, a_n$ 与 $b_1, \cdots, b_n$ 中属于 P 的非零元个数分别为 r 与 s. 不妨设 $0 <_P a_i$, $i = 1, \cdots, r$, 但 $a_i \leqslant_P 0$, $i = r+1, \cdots, n$; 同时 $0 <_P b_j$, $j = 1, \cdots, s$, 但 $b_j \leqslant_P 0$, $j = s+1, \cdots, n$. 由于 $q \approx_F \varrho$, 从而有非退化的线性替换，使得下面等式成立：

$$a_1x_1^2+\cdots+a_nx_n^2=b_1y_1^2+\cdots+b_ny_n^2.$$

令 $C=(c_{ij})_{n\times n}$ 是该线性替换的系数矩阵，则 C 是 F 上 n 阶可逆矩阵. 假设 $r>s$. 由线性方程组理论知，如下方程组

$$\begin{cases} c_{i1}x_1+\cdots+c_{in}x_n=0, & i=1,\cdots,s \\ x_{r+1}=\cdots=x_n=0 \end{cases}$$

在 F 中有非零解 $(d_1,\cdots,d_r,0,\cdots,0)$.

将 $(x_1,\cdots,x_n)=(d_1,\cdots,d_r,0,\cdots,0)$ 代入上面等式，则有 $a_1d_1^2+\cdots+a_rd_r^2=b_{s+1}e_{s+1}^2+\cdots+b_ne_n^2\in P\cap -P=\{0\}$, 其中 $e_j=c_{j1}d_1+\cdots+c_{jr}d_r$, $j=s+1,\cdots,n$. 由此可推出，$d_1=\cdots=d_r=0$, 矛盾. 于是，$r\leqslant s$. 同理可证，$s\leqslant r$. 因而 $r=s$. 由此有 $\mathrm{sgn}_P(q)=r-(\mathrm{rank}(q)-r)=s-(\mathrm{rank}(\varrho)-s)=\mathrm{sgn}_P(\varrho)$. 证毕.

根据上面定理，下面的定义是合理的.

定义 5.5.5 设 q 是域 F 上一个型，且 $q\approx_F\langle a_1,\cdots,a_n\rangle$. 对于 F 的任意半锥 P, $\mathrm{sgn}_P(\langle a_1,\cdots,a_n\rangle)$ 称作型 q 关于 P 的符号差，且记作 $\mathrm{sgn}_P(q)$.

此外，作为迷向型与反迷向型的一种衍变，我们给出如下定义.

定义 5.5.6 域 F 的一个正则型 q 称作在 F 上是强反迷向的，如果对于每个自然数 n, $n\times q=q\oplus q\oplus\cdots\oplus q$ 在 F 上是反迷向的. 否则，即对于某个自然数 m, $m\times q$ 在 F 上是迷向的，称 q 在 F 上是弱迷向的.

显然，强反迷向的型是反迷向的，而迷向型必是弱迷向的. 若 P 是域 F 的一个半锥，则对于任意有限个非零元 $a_1,\cdots,a_n\in P$, 型 $\langle a_1,\cdots,a_n\rangle$ 在 F 上是强反迷向的. 此外，若 q 和 ϱ 都是域 F 上的型，且 $q\approx_F\varrho$, 则 q 在 F 上是强反迷向的(弱迷向的)，当且仅当 ϱ 是强反迷向的 (弱迷向的).

作为二次型的弱迷向性的一个简单判别，我们可建立下面命题.

命题 5.5.9 设 q 是实域 F 上一个正则型，且 $q\approx_F\langle a_1,\cdots,a_n\rangle$, 则 q 在 F 上是弱迷向的，当且仅当有不全为零的 $s_1,\cdots,s_n\in S_F$, 使得 $\sum\limits_{i=1}^n a_is_i=0$.

证明 设对于某个自然数 m, $m\times q$ 在 F 上是迷向的，则 $m\times\langle a_1,\cdots,a_n\rangle$ 也是迷向的. 从而有不全为零 $b_{ij}\in F$, $i=1,\cdots,n$; $j=1,\cdots,m$, 使得 $\sum\limits_{i=1}^n a_i\left(\sum\limits_{j=1}^m b_{ij}^2\right)=0$.

令 $s_i=\sum\limits_{j=1}^m b_{ij}^2\in S_F$, $i=1,\cdots,n$. 由于 F 是实域，从而 $s_1,\cdots,s_n$ 也不全为零.

此时，$\sum\limits_{i=1}^n a_is_i=0$.

反过来，设 $\sum_{i=1}^{n} a_i s_i = 0$, 其中 $s_1, \cdots, s_n \in S_F$, 且它们不全为零. 令 m 是 $s_1, \cdots, s_n$ 中平方项的最大个数，则可写作： $s_i = \sum_{j=1}^{m} b_{ij}^2$, 其中 $b_{ij} \in F$, $i = 1, \cdots, n$; $j = 1, \cdots, m$. 此时易知， $m \times \langle a_1, \cdots, a_n \rangle$ 即 $m \times q$ 是在 F 上迷向的. 证毕.

下面命题表明，"强反迷向" 与 "弱迷向" 这两个概念仅对实域才有实质上意义.

命题 5.5.10 若域 F 不是实域，则 F 上每个型都是弱迷向的.

证明 设 $-1 = \sum_{i=1}^{m} b_i^2$, 其中 $b_i \in F$, $i = 1, \cdots, m$, 则易知，对于每个型 q, $(m+1) \times q$ 是迷向的. 证毕.

考虑到，"半序" 是 "序" 在概念上的一个相近事物. 因而，给出下列定义是很自然的.

定义 5.5.7 设 P 是域 F 的一个半锥，q 是 F 上一个 n 维正则型. 若 $\mathrm{sgn}_P(q) = n$ $(\mathrm{sgn}_P(q) = -n)$, 则称 q 关于 P 是正定的 (负定的). 如果 q 关于 P 既不是正定的又不是负定的，那么称 q 关于 P 是不定的.

定理 5.5.11 设 q 是域 F 上一个正则型，则 q 在 F 上是弱迷向的，当且仅当对于 F 的每个半锥 P, q 关于 P 是不定的.

证明 必要性：设 q 在 F 上是弱迷向的，则对于某个自然数 m, $m \times q$ 是迷向的. 此时，对于 F 的每个半锥 P, $m \times q$ 关于 P 只可能是不定的. 注意到 $\mathrm{sgn}_P(m \times q) = m \cdot \mathrm{sgn}_P(q)$. 从而， q 关于 P 是不定的.

充分性：设 q 在 F 上是强反迷向的，且令 $q \approx_F \langle a_1, \cdots, a_n \rangle$, 其中 $a_i \in \dot{F}$, $i = 1, \cdots, n$. 考虑 F 的如下非空子集：

$$T = \left\{ \sum_{i=1}^{n} a_i s_i^2 \mid s_i \in S_F, i = 1, \cdots, n \right\}.$$

由于 q 在 F 上不是弱迷向的，从而易验证， T 是 F 的一个亚半锥. 由定义可知， $-T$ 也是 F 的一个亚半锥. 如果 $1 \notin T$, 则 $-1 \notin -T$. 由引理 5.5.1 知， $-T + S_F$ 是 F 的一个包含 1 的亚半锥. 因此， T 或 $-T + S_F$ 是 F 的一个包含 1 的亚半锥. 由定理 5.5.2 知， F 有一个半锥 P, 使得 $T \subseteq P$ 或 $-T + S_F \subseteq P$. 当 $T \subseteq P$ 时， $a_i \in T \subseteq P$, $i = 1, \cdots, n$; 当 $-T + S_F \subseteq P$ 时， $-a_i \in -T \subseteq -T + S_F \subseteq P$, $i = 1, \cdots, n$. 这表明 q 关于 P 是正定或负定的. 从而充分性获证.

为今后的进一步讨论，再引入如下定义.

定义 5.5.8 称一个域 F 满足弱 Hasse 原理，如果对于 F 上每个正则型 q, 只要 q 对于 F 的每个序 (正锥) 都是不定的， q 在 F 上必是弱迷向的. 此时，简称域 F 满足 WH.

定理 5.5.12 对于一个域 F, 下列叙述是等价的:

(1) 域 F 满足 WH;

(2) F 的每个半序是序;

(3) 对于任意 $a, b \in \dot{F}$, 型 $\langle 1, a, b, -ab\rangle$ 是弱迷向的.

证明 (1) $\Longrightarrow$ (3): 对于 F 的每个序 P, 型 $\langle 1, a, b, -ab\rangle$ 显然是不定的. 由叙述 (1) 知, $\langle 1, a, b, -ab\rangle$ 是弱迷向的.

(3) $\Longrightarrow$ (2): 设 $\leqslant$ 是 F 的任意半序, 且 $0 < a$, $0 < b$. 由叙述 (3) 知, 型 $\langle 1, a, b, -ab\rangle$ 是弱迷向的. 此时必有 $-ab < 0$, 即 $0 < ab$. 这表明: $\leqslant$ 是 F 的一个序.

(2) $\Longrightarrow$ (1): 由定理 5.5.11 即得. 证毕.

§5.6 半序空间和 Baer-Krull 定理

在本节中, 我们将沿着关于序的讨论途径来研究半序, 比如半序空间的拓扑, 半序和实赋值之间的相容性等. 然后, 我们研究与给定实赋值相容的半序的构造形式, 由此建立重要的 Baer-Krull 定理.

设 F 是一个域, 且记 $\mathcal{Y}_F$ 为 F 的所有半锥组成的集合. 由定理 5.5.2 及其推论可知, $\mathcal{Y}_F \neq \varnothing$ 当且仅当 F 是实域. 此外, 显然 $\mathcal{X}_F \subseteq \mathcal{Y}_F$, 这里 $\mathcal{X}_F$ 是域 F 的序空间.

对于 $a \in \dot{F}$, 可类似地规定 $\mathcal{Y}_F$ 的如下子集:

$$H_Y(a) = \{P \in \mathcal{Y}_F \mid a \in P\}.$$

同样, 容易验证, 子集族 $\{H_Y(a) \mid a \in \dot{F}\}$ 组成 $\mathcal{Y}_F$ 的一个拓扑子基.

定义 5.6.1 由上面子集族 $\{H_Y(a) \mid a \in \dot{F}\}$ 作为 $\mathcal{Y}_F$ 的子基所生成的拓扑称作 $\mathcal{Y}_F$ 的 Harrison 拓扑. 此时, 具有 Harrison 拓扑的拓扑空间 $\mathcal{Y}_F$ 称作域 F 的半序空间.

显然, 半序空间 $\mathcal{Y}_F$ 的每个基本开集可表为 $H_Y(a_1, \cdots, a_n) := \bigcap_{i=1}^{n} H_Y(a_i)$, 其中 $a_i \in \dot{F}$, $i = 1, \cdots, n$. 由域 F 的序空间 $\mathcal{X}_F$ 的拓扑结构知, 序空间 $\mathcal{X}_F$ 实际上是 $\mathcal{Y}_F$ 的一个子空间. 设 $P \in \mathcal{Y}_F$, 但 $P \notin \mathcal{X}_F$, 则对于某两个 $a, b \in P$, $ab \notin P$. 此时有 $P \in H_Y(a, b, -ab)$, 但 $H_Y(a, b, -ab) \cap \mathcal{X}_F = \varnothing$. 因此, $\mathcal{X}_F$ 还是 $\mathcal{Y}_F$ 的闭子集.

照搬定理 1.5.3 的证明, 可建立下面的定理.

定理 5.6.1 设 F 是一个实域, 则 F 的半序空间是一个全不连通的 Hausdorff 紧空间.

完全类似于定义 3.1.3, 我们可引进如下定义.

定义 5.6.2 设 $\leqslant$ 是域 F 的一个半序，v 是 F 的一个赋值. 称 v 和半序 $\leqslant$ 相容，若由关系式 $0 < a \leqslant b$ 可推出 $v(a) \geqslant v(b)$. 此时，亦称 v 与半锥 P 相容，这里 P 是半序 $\leqslant$ 的对应半锥.

同样，可建立下面结论.

命题 5.6.2 设 v 是域 F 的一个赋值，A_v 和 M_v 分别是 v 的赋值环和赋值理想，且 $\leqslant$ 是 F 的一个半序，则对于如下叙述:

(1) v 与 $\leqslant$ 相容;

(2) A_v 关于 $\leqslant$ 是凸的;

(3) M_v 关于 $\leqslant$ 是凸的;

(4) 对于每个 $a \in M_v$, $a < 1$,

蕴含关系: (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) $\Longrightarrow$ (4) 成立.

证明 根据命题 5.5.3 可知，定理 3.1.3 中相应的蕴含关系的证明同样适合半序. 因此，上面命题成立. 证毕.

在后面，将有例子表明，蕴含关系 "(4) $\Longrightarrow$ (1)" 在一般情况下对于半序是不成立的.

推论 设 v 是域 F 的一个赋值，且 v 与 F 的一个半序 $\leqslant$ 相容，则 v 是 F 的一个实赋值.

证明 设 M_v 是 v 的赋值理想，且 $a_1^2+\cdots+a_n^2 \in M_v$, 则显然有 $0 \leqslant a_j^2 \leqslant a_1^2+\cdots+a_n^2 \in M_v$, $j=1,\cdots,n$. 由命题 5.6.2 知，M_v 关于 $\leqslant$ 是凸的. 从而 $a_j^2 \in M_v$, 即 $a_j \in M_v$, $j=1,\cdots,n$. 根据命题 3.1.2, v 是 F 的一个实赋值. 证毕.

设 v 是域 F 的一个实赋值，则可引进半序空间 $\mathcal{Y}_F$ 的如下子集:

$$\mathcal{Y}_F^v = \{P \in \mathcal{Y}_F \mid v \text{ 与 } P \text{ 相容 }\}.$$

显然，$\mathcal{X}_F^v \subseteq \mathcal{Y}_F^v$, 这里 $\mathcal{X}_F^v$ 是 F 的所有与 v 相容的正锥 (序) 组成的集合. 设 $P \in \mathcal{Y}_F$, 但 $P \notin \mathcal{Y}_F^v$, 则由定义 5.6.2 知，有 $a, b \in F$, 使得 $0 <_P a \leqslant_P b$, 但 $v(a) < v(b)$. 此时，显然 $P \in H_Y(a, b-a)$, 但 $H_Y(a, b-a) \cap \mathcal{Y}_F^v = \varnothing$. 因此，$\mathcal{Y}_F^v$ 是半序空间 $\mathcal{Y}_F$ 的闭子集.

为了刻画 $\mathcal{Y}_F^v$ 和 $\mathcal{X}_F^v$ 的成员，我们需要下面的定义.

定义 5.6.3 设 v 是域 F 的一个赋值，G_v 是 v 的值群. v 的一个半截口是 G_v 到 $\dot{F}$ 的一个映射 s, 使得下列条件成立: (1)$s(0)=1$; (2) 对于每个 $g \in G_v$, $v(s(g))=g$; (3) 对于 $g_1, g_2 \in G_v$, $s(g_1+g_2) \in s(g_1)s(g_2)\dot{F}^2$.

注 (1) 显然，对于 $g \in G_v$, $s(2g) \in \dot{F}^2$. 由此有，当 $g_1 - g_2 \in 2G_v$ 时，$s(g_1)s^{-1}(g_2) \in \dot{F}^2$.

(2)v 的一个半截口 s 称作一个截口，若对于 $g_1, g_2 \in G_v$, $s(g_1+g_2)=s(g_1)s(g_2)$.

例如，当 $G_v = \mathbb{Z}$ 时，选取 $a \in \dot{F}$, 使得 $v(a) = 1$, 且规定 $s(m) = a^m$, 其中 $m \in \mathbb{Z}$. 此时，所规定的 s 是 v 的一个截口.

对于域 F 的任意一个赋值 v, v 的截口未必存在. 然而， v 的半截口总是存在的. 在下面讨论中，对于域 F 的一个赋值 v, v 的值群、赋值环、赋值理想和剩余域总记作 G, A, M 和 F_v.

命题 5.6.3 域 F 的每个赋值 v 都有半截口.

证明 设 G 是 v 的值群. 注意到，商群 $G/2G$ 可看作二元域 $\mathbb{Z}/2\mathbb{Z}$ 上一个向量空间. 从而 G 有一个子集 B, 使得 $\{g + 2G \mid g \in B\}$ 组成向量空间 $G/2G$ 的一个基.

对于每个非零 $g \in G$, 任意取定 $a_g \in \dot{F}$, 使得 $v(a_g) = g$. 同时，对于 $0 \in G$, 规定 $a_0 = 1$.

对于任意 $g \in G$, g 可惟一地表为

$$g = g_1 + \cdots + g_n + 2g_0,$$

其中 n 为非负整数， $g_0 \in G$, 且 $g_1, \cdots, g_n \in B$.

据此规定 $s(g) = a_{g_0}^2 a_{g_1} \cdots a_{g_n}$. 容易验证：所规定的映射 s: $G \longrightarrow \dot{F}$ 是 v 的一个半截口. 证毕.

引理 5.6.4 设 v 是域 F 的一个赋值， v 的值群、赋值环、赋值理想与剩余域分别记作 G, A, M 与 F_v, 且 s 是 v 的一个半截口，则 $\mathcal{Y}_F^v$ 中每个半序 P 诱导出如下一对映射：

(1) $\sigma_P: \ G/2G \longrightarrow \{1, -1\}$, 使得对于每个 $\bar{g} := g + 2G \in G/2G$, 其中 $g \in G$, $\sigma_P(\bar{g}) = 1$, 若 $s(g) \in P$; 否则 $\sigma_P(\bar{g}) = -1$. 特别地， $\sigma_P(\bar{0}) = 1$.

(2) $\mathcal{P}_P: \ G/2G \longrightarrow \mathcal{Y}_{F_v}$, 使得对于每个 $\bar{g} := g + 2G \in G/2G$, 其中 $g \in G$, $\mathcal{P}_P(\bar{g}) = \{b + M \mid b \in A \setminus M$, 使得 $bs(g)\sigma_P(\bar{g}) \in P\} \cup \{0 + M\}$.

证明 (1) 若 $\bar{g}_1 = \bar{g}_2$, 则 $g_1 - g_2 \in 2G$. 由定义 5.6.3 后的注， $s(g_1)s(g_2)^{-1} \in \dot{F}^2$. 从而 $s(g_1) \in P$, 当且仅当 $s(g_2) \in P$. 因此，映射 σ_P 是合理的.

(2) 注意到， $s(g)\sigma_P(\bar{g}) \in P$, 从而 $\bar{1} := 1 + M \in \mathcal{P}_P(\bar{g})$. 容易证明： $\mathcal{P}_P(\bar{g}) + \mathcal{P}_P(\bar{g}) \subseteq \mathcal{P}_P(\bar{g})$, $F_v^2 \cdot \mathcal{P}_P(\bar{g}) \subseteq \mathcal{P}_P(\bar{g})$, 且 $F_v = \mathcal{P}_P(\bar{g}) \cup -\mathcal{P}_P(\bar{g})$. 此外，假设 $\bar{b} = b + M \in \mathcal{P}_P(\bar{g}) \cap -\mathcal{P}_P(\bar{g})$, 且 $b \notin M$, 则存在 $b_1, b_2 \in b + M$, 使得 $b_1 s(g)\sigma_P(\bar{g})$, $-b_2 s(g)\sigma_P(\bar{g}) \in P$. 由此有 $0 <_P b_1 s(g)\sigma_P(\bar{g}) <_P (b_1 - b_2)s(g)\sigma_P(\bar{g})$. 由于 v 与 p 是相容的，从而 $v(b_1 s(g)\sigma_P(\bar{g})) \geqslant v((b_1 - b_2)s(g)\sigma_P(\bar{g}))$. 于是， $v(b_1) \geqslant v(b_1 - b_2) > 0$, 即 $b_1 \in M$. 于是 $b + M = b_1 + M = \bar{0}$, 与假设矛盾. 因而， $\mathcal{P}_P(\bar{g}) \cap -\mathcal{P}_P(\bar{g}) = \{\bar{0}\}$. 因此， $\mathcal{P}_P(\bar{g}) \in \mathcal{Y}_{F_v}$. 证毕.

引理 5.6.5 设 v 是域 F 的一个实赋值， v 的值群、赋值环、赋值理想和剩余域分别为 G, A, M 和 F_v, 且 s 是 v 的一个半截口，则对于任意映射 $\mathcal{P}$: $G/2G \longrightarrow \mathcal{Y}_{F_v}$

以及任意映射 σ: $G/2G \longrightarrow \{1,-1\}$, 其中 $\sigma(\bar{0})=1$, $\mathcal{P}$ 和 σ 确定 $\mathcal{Y}_F^v$ 中如下半锥.

$$\mathcal{P}^\sigma=\{a\in F\mid a=0 \text{ 或 } \frac{a}{s(v(a))}\sigma(\overline{v(a)})+M\in\mathcal{P}(\overline{v(a)})\}.$$

证明 下面根据定义验证: $\mathcal{P}^\sigma$ 是 F 的一个与 v 相容的半锥.

(1) 设非零的 $a, b\in\mathcal{P}^\sigma$, 则有

$$\text{(i)} \qquad 0\neq\frac{a}{s(v(a))}\sigma(\overline{v(a)})+M\in\mathcal{P}(\overline{v(a)})$$

且

$$\text{(ii)} \qquad 0\neq\frac{b}{s(v(b))}\sigma(\overline{v(b)})+M\in\mathcal{P}(\overline{v(b)}).$$

下面分情况讨论.

情况 1 $v(a)=v(b)$. 此时由 (i) 和 (ii) 有

$$0\neq\frac{(a+b)}{s(v(a))}\sigma(\overline{v(a)})+M\in\mathcal{P}(\overline{v(a)}).$$

这表明 $\frac{(a+b)}{s(v(a))}\in A\setminus M$. 从而 $v\Big(\frac{(a+b)}{s(v(a))}\Big)=0$, 即有 $v(a+b)=v(a)$. 于是有 $\frac{(a+b)}{s(v(a+b))}\sigma(\overline{v(a+b)})+M\in\mathcal{P}(\overline{v(a+b)})$. 从而 $a+b\in\mathcal{P}^\sigma$.

情况 2 $v(a)<v(b)$. 此时, $v(a+b)=v(a)$, 且 $\frac{(a+b)}{s(v(a+b))}\sigma(\overline{v(a+b)})+M=\frac{(a+b)}{s(v(a))}\sigma(\overline{v(a)})+M=\frac{a}{s(v(a))}\sigma(\overline{v(a)})+M$. 由 (i) 式即有 $a+b\in\mathcal{P}^\sigma$.

情况 3 $v(b)<v(a)$. 此时, 类似于情况 2 可得 $a+b\in\mathcal{P}^\sigma$.

(2) 设非零 $a\in\mathcal{P}^\sigma$, 且 $b\in\dot{F}$. 此时, 上面的关系式 (i) 成立. 由于 $v(ab^2)=v(a)+2v(b)$, 从而 $\overline{v(ab^2)}=\overline{v(a)}$. 显然 $s(v(ab^2))=s(v(a))s(v(b))^2\xi^2$, 这里 $\xi\in A\setminus M$. 于是有

$$\begin{aligned}&\frac{ab^2}{s(v(ab^2))}\sigma(\overline{v(ab^2)})+M\\ =\;&\left(\frac{b}{s(v(b))}\xi^{-1}+M\right)^2\left(\frac{a}{s(v(a))}\sigma(\overline{v(a)})+M\right)\\ \in\;&F_v^2\cdot\mathcal{P}(\overline{v(a)})\subseteq\mathcal{P}(\overline{v(a)})=\mathcal{P}(\overline{v(ab^2)})\end{aligned}$$

从而 $ab^2\in\mathcal{P}^\sigma$. 此外, 由于 $s(0)=1$ 且 $\sigma(\bar{0})=1$, 从而显然有 $1\in\mathcal{P}^\sigma$.

(3) 假设 $a\in\mathcal{P}^\sigma\cap-\mathcal{P}^\sigma$, 且 $a\neq0$, 则有 $\frac{a}{s(v(a))}\sigma(\overline{v(a)})+M\in\mathcal{P}(\overline{v(a)})\cap-\mathcal{P}(\overline{v(a)})$. 从而有 $\frac{a}{s(v(a))}\sigma(\overline{v(a)})\in M$; 这是不可能的. 因而, $\mathcal{P}^\sigma\cap-\mathcal{P}^\sigma=\{0\}$.

(4) 显然有 $F=\mathcal{P}^\sigma\cup-\mathcal{P}^\sigma$. 证毕.

由上面两个引理，可以建立下面的定理.

定理 5.6.6 设 v 是域 F 的一个实赋值，v 的值群、赋值环、赋值理想和剩余域分别为 G, A_v, M_v 和 F_v, s 是 v 的一个半截口，记 $M(G/2G,\mathcal{Y}_{F_v})$ 为商群 $G/2G$ 到 $\mathcal{Y}_{F_v}$ 的全体映射组成的集合，且 $\sigma(G/2G,\{1,-1\})$ 为 $G/2G$ 到 $\{1,-1\}$ 的所有使得 $\sigma(\bar{0})=1$ 的映射 σ 组成的集合，则存在 $\mathcal{Y}_F^v$ 到 $\sigma(G/2G,\{1,-1\})\times M(G/2G,\mathcal{Y}_{F_v})$ 的如下双射：

$$\phi:\quad P\longmapsto(\sigma_P,\mathcal{P}_P),\ \text{对于每个}\ P\in\mathcal{Y}_F,$$

这里，σ_P 和 $\mathcal{P}_P$ 的规定如引理 5.6.4. 并且上面映射的逆映射恰为

$$\psi:\quad(\sigma,\mathcal{P})\longmapsto\mathcal{P}^\sigma,\ \text{对于}\ \sigma\in\sigma(G/2G,\{1,-1\}),\ \mathcal{P}\in M(G/2G,\mathcal{Y}_{F_v}),$$

其中 $\mathcal{P}^\sigma$ 的规定如引理 5.6.5.

证明 先证：对于每个 $P\in\mathcal{Y}_F^v$, $\psi\circ\phi(P)=P$. 设 $a\in\psi\circ\phi(P)=\mathcal{P}_P^{\sigma_P}$, 则 $\dfrac{a}{s(v(a))}\sigma_P(\overline{v(a)})+M_v\in\mathcal{P}_P(\overline{v(a)})$. 由 $\mathcal{P}_P$ 的规定有

$$\frac{a}{s(v(a))}\sigma_P(\overline{v(a)})s(v(a))\sigma_P(\overline{v(a)})\in P.$$

由此有 $a\in P$. 从而 $\mathcal{P}_P^{\sigma_P}\subseteq P$, 必定 $\mathcal{P}_P^{\sigma_P}=P$.

再证：对于任意 $\mathcal{P}\in M(G/2G,\mathcal{Y}_{F_v})$ 以及 $\sigma\in\sigma(G/2G,\{1,-1\})$, $\phi\circ\psi(\sigma,\mathcal{P})=(\sigma,\mathcal{P})$, 即 $\sigma_{\mathcal{P}_\sigma}=\sigma$ 且 $\mathcal{P}_{\mathcal{P}^\sigma}=\mathcal{P}$. 由规定，对于 $\bar{g}=g+2G\in G/2G$, $\sigma_{\mathcal{P}^\sigma}(\bar{g})s(g)\in\mathcal{P}^\sigma$. 进而有 $\dfrac{\sigma_{\mathcal{P}^\sigma}(\bar{g})s(g)}{s(v(\sigma_{\mathcal{P}^\sigma}(\bar{g})s(g)))}\sigma(\overline{v(\sigma_{\mathcal{P}^\sigma}(\bar{g})s(g))})+M_v\in\mathcal{P}(\overline{v(\sigma_{\mathcal{P}^\sigma}(\bar{g})s(g))})$, 即 $\sigma_{\mathcal{P}^\sigma}(\bar{g})\sigma(\bar{g})\in\mathcal{P}(\bar{g})$. 注意到，$\sigma_{\mathcal{P}^\sigma}(\bar{g})\sigma(\bar{g})=1$ 或 -1. 从而必有 $\sigma_{\mathcal{P}^\sigma}(\bar{g})\sigma(\bar{g})=1$, 即 $\sigma_{\mathcal{P}^\sigma}(\bar{g})=\sigma(\bar{g})$. 由 $\bar{g}$ 的任意性知，$\sigma_{\mathcal{P}^\sigma}=\sigma$.

再设 $b+M_v\in\mathcal{P}_{\mathcal{P}^\sigma}(\bar{g})$, 其中 $b\in A_v\setminus M_v$, 且 $\bar{g}=g+2G\in G/2G$. 由规定知，$bs(g)\sigma_{\mathcal{P}^\sigma}(\bar{g})\in\mathcal{P}^\sigma$, 即 $bs(g)\sigma(\bar{g})\in\mathcal{P}^\sigma$. 由此有

$$\frac{bs(g)\sigma(\bar{g})}{s(v(bs(g)\sigma(\bar{g})))}\sigma(\overline{v(bs(g)\sigma(\bar{g}))})+M_v\in\mathcal{P}(\overline{v(bs(g)\sigma(\bar{g}))}).$$

上式即为 $b+M_v\in\mathcal{P}(\bar{g})$. 从而有 $\mathcal{P}_{\mathcal{P}^\sigma}(\bar{g})\subseteq\mathcal{P}(\bar{g})$. 此时必有 $\mathcal{P}_{\mathcal{P}^\sigma}(\bar{g})=\mathcal{P}(\bar{g})$. 由 $\bar{g}$ 的任意性知，$\mathcal{P}_{\mathcal{P}^\sigma}=\mathcal{P}$. 证毕.

上面集合 $\sigma(G/2G,\{1,-1\})$ 中的映射 σ 称作一个特征标，若 σ 是商群 $G/2G$ 到乘法群 $\{1,-1\}$ 的一个同态. 记 $\mathrm{Hom}(G/2G,\{1,-1\})$ 为 $G/2G$ 到 $\{1,-1\}$ 的所有特征标组成的集合.

定理 5.6.7 记号同定理 5.6.6, 则 $P\in\mathcal{X}_F^v$, 当且仅当 $\mathcal{P}_P$ 为 $G/2G$ 到 $\mathcal{X}_F^v$ 的一

个常量函数，且 $\sigma_P \in \mathrm{Hom}(G/2G, \{1, -1\})$.

证明 先设 $P \in \mathcal{X}_F^v$. 对于 g_1, $g_2 \in G$, 令 $e = \sigma_P(\bar{g}_1 + \bar{g}_2)$, 其中 $e = 1$ 或 -1. 由 σ_P 的规定，有 $es(g_1 + g_2) \in P$, 即有 $es(g_1)s(g_2) \in P$. 由于 $P \in \mathcal{X}_F^v$, 从而有 $es(g_1)$, $s(g_2) \in P$, 或者 $es(g_1)$, $s(g_2) \in -P$. 于是总有 $e\sigma_P(\bar{g}_1)\sigma_P(\bar{g}_2) = 1$，即 $\sigma_P(\bar{g}_1)\sigma_P(\bar{g}_2) = e = \sigma_P(\bar{g}_1 + \bar{g}_2)$. 因而， $\sigma_P \in \mathrm{Hom}(G/2G, \{1, -1\})$.

对于任意 $\bar{g} = g + 2G \in G/2G$, 设 $b + M_v \in \mathcal{P}_P(\bar{g})$, 其中 $b \in A_v \setminus M_v$. 由 $\mathcal{P}_P(\bar{g})$ 的规定知， $bs(g)\sigma_P(\bar{g}) \in P$. 注意到 $s(g)\sigma_P(\bar{g}) \in P$ 且不为零. 从而 $b \in P$, 即 $bs(0)\sigma_P(\bar{0}) \in P$. 于是有 $b + M_v \in \mathcal{P}_P(\bar{0})$. 这表明 $\mathcal{P}_P(\bar{g}) \subseteq \mathcal{P}_P(\bar{0})$. 此时，必有 $\mathcal{P}_P(\bar{g}) = \mathcal{P}_P(\bar{0})$. 此外，根据命题 3.1.3 的推论， $\mathcal{P}_P(\bar{0})$ 为 F_v 的一个正锥.

反过来, 设 $\sigma_P \in \mathrm{Hom}(G/2G, \{1.-1\})$, 且对于任意 $g \in G$, $\mathcal{P}_P(\bar{g}) = \mathcal{P}_P(\bar{0}) \in \mathcal{X}_{F_v}$. 若 a_1, a_2 是 P 中非零元素，则由 $P = \mathcal{P}_P^{\sigma_P}$ 知,

$$\frac{a_i}{s(v(a_i))}\sigma_P(\overline{v(a_i)}) + M_v \in \mathcal{P}_P(\overline{v(a_i)}) = \mathcal{P}_P(\bar{0}), \quad i = 1, 2.$$

由此有

$$\frac{a_1 a_2}{s(v(a_1))s(v(a_2))}\sigma_P(\overline{v(a_1)})\sigma_P(\overline{v(a_2)}) + M_v \in \mathcal{P}_P(\bar{0}).$$

注意到 $s(v(a_1 a_2)) = s(v(a_1) + v(a_2)) = s(v(a_1))s(v(a_2))\xi^2$, 其中 $\xi \in A_v \setminus M_v$. 从而可得

$$\frac{a_1 a_2}{s(v(a_1 a_2))}\sigma_P(\overline{v(a_1 a_2)}) + M_v \in \mathcal{P}_P(\bar{0}) = \mathcal{P}_P(\overline{v(a_1 a_2)}).$$

这表明 $a_1 a_2 \in \mathcal{P}_P^{\sigma_P} = P$. 因而， $P \in \mathcal{X}_F^v$. 证毕.

推论 1(Baer-Krull) 设 v 是域 F 的一个实赋值, 则存在 $\mathcal{X}_F^v$ 到 $\mathcal{X}_{F_v} \times \mathrm{Hom}(G/2G, \{1, -1\})$ 的如下双射:

$$P \longmapsto (\overline{P}, \sigma_P),$$

其中 σ_P 的规定同上， $\overline{P}$ 为 P 在剩余域 F_v 上所诱导的正锥.

证明 注意到 $\mathcal{P}_P(\bar{0})$ 恰为 P 在 F_v 上所诱导的正锥，从而即有结论.

推论 2 设 v 是 F 的一个实赋值，则 $\mathcal{X}_F^v = \mathcal{Y}_F^v$, 当且仅当 $|G/2G| = 2$ 与 $|\mathcal{X}_{F_v}| = 1$, 或者 $|G/2G| = 1$ 与 $\mathcal{X}_{F_v} = \mathcal{Y}_{F_v}$.

证明 任意取定 v 的一个半截口 s.

充分性：由条件 $|G/2G| \leqslant 2$ 可知, $\sigma(G/2G, \{1, -1\})$ 中每个元素都是特征标. 此外，由定理 5.5.2 的推论 3 知，当 $|\mathcal{X}_{F_v}| = 1$ 时， $\mathcal{X}_{F_v} = \mathcal{Y}_{F_v}$. 因而，在所给的两种情况下， $M(G/2G, \mathcal{Y}_{F_v})$ 中每个映射都是 $G/2G$ 到 $\mathcal{X}_{F_v}$ 的常量映射. 由定理 5.6.6 和定理 5.6.7 知， $\mathcal{X}_F^v = \mathcal{Y}_F^v$.

必要性：假若 $|G/2G| > 2$, 则易知这样一个事实： $\mathrm{Hom}(G/2G, \{1,-1\})$ 是 $\sigma(G/2G, \{1,-1\})$ 的真子集．由定理 5.6.6 和定理 5.6.7 可知， F 有一个真半锥属于 $\mathcal{Y}_F^v$, 即 $\mathcal{X}_F^v \neq \mathcal{Y}_F^v$, 矛盾于所设．从而， $|G/2G| = 1$ 或 2. 假若 $|G/2G| = 2$, 但 $|\mathcal{X}_{F_v}| > 1$, 则 $M(G/2G, \mathcal{Y}_{F_v})$ 中显然有非常量映射．由定理 5.6.6 和定理 5.6.7 又可推出矛盾： $\mathcal{X}_F^v \neq \mathcal{Y}_F^v$. 因而，当 $|G/2G| = 2$ 时，必有 $|\mathcal{X}_{F_v}| = 1$. 当 $|G/2G| = 1$ 时，假若 $\mathcal{X}_{F_v} \neq \mathcal{Y}_{F_v}$, 则 $M(G/2G, \mathcal{Y}_{F_v})$ 中有一个映射 $\mathcal{P}$, 使得 $\mathcal{P}(\bar{0})$ 为 F_v 的真半锥．由此可得 $\mathcal{X}_F^v \neq \mathcal{Y}_F^v$, 矛盾．因而，当 $|G/2G| = 1$ 时，必有 $\mathcal{X}_{F_v} = \mathcal{Y}_{F_v}$. 证毕.

借助于定理 5.6.6 和定理 5.6.7, 很容易构造一个真半序的例子.

例　设 $F = \mathbb{Q}(\sqrt{2})(t)$, 这里 t 是数域 $\mathbb{Q}(\sqrt{2})$ 上一个未定元．由命题 3.1.1(2) 知, F 有一个赋值 v, 使得对于每个非零多项式 $f(t) \in \mathbb{Q}(\sqrt{2})[t]$, $v(f(t)) = -\deg f(t)$, v 的值群 $G_v = \mathbb{Z}$, 且 v 的剩余域 $F_v \cong \mathbb{Q}(\sqrt{2})$. 由于 $\mathbb{Q}$ 仅有惟一正锥，从而由定理 2.3.7 知，域 $\mathbb{Q}(\sqrt{2})$ 有两个相异正锥．于是 F_v 有两个相异正锥： P_1, P_2. 注意到 $G_v/2G_v = \{\bar{0}, \bar{1}\}$, 且规定 $\mathcal{P}(\bar{0}) = P_1$, 而 $\mathcal{P}(\bar{1}) = P_2$. 此外，规定 $\sigma(\bar{0}) = \sigma(\bar{1}) = 1$. 根据定理 5.6.6 和定理 5.6.7 知， $\mathcal{P}^\sigma$ 是域 F 的一个真半锥.

§5.7　半序及其凸赋值环

由上节的命题 5.6.2 知，对于域 F 的一个半序 $\leqslant$ 以及一个实赋值 v, 若 v 与 $\leqslant$ 相容，则 v 的赋值环 A_v 关于 $\leqslant$ 是凸的．然而，这一结论的逆命题是不成立的．因此，与 $\leqslant$ 相容的实赋值和关于 $\leqslant$ 凸的赋值环之间不存在一一对应．这一现象也反映"序"与"半序"之间的差异．在本节中，我们将讨论关于某个半序是凸的赋值环的构造，同时建立与半序和实赋值有关的一些结果.

首先，应该注意的是如下事实.

命题 5.7.1　设 $\leqslant$ 是域 F 的一个半序，则 F 的每个关于 $\leqslant$ 凸的赋值环都是实赋值环.

证明　设 A 是 F 的一个关于 $\leqslant$ 凸的赋值环，且 v 和 M 分别为 A 的对应的赋值和 A 的极大理想．由命题 5.6.2 知， M 关于 $\leqslant$ 是凸的．设 $a_1^2 + \cdots + a_n^2 \in M$, 其中 $a_1, \cdots, a_n \in A$, 则 $0 \leqslant a_i^2 \leqslant a_1^2 + \cdots + a_n^2 \in M$, $i = 1, \cdots, n$. 由 M 的凸性有 $a_i^2 \in M$, 即 $a_i \in M$, $i = 1, \cdots, n$. 根据命题 3.1.2 知， v 是 F 的一个实赋值，即 A 是 F 的一个实赋值环．证毕.

设 $\leqslant$ 是域 F 的一个半序， E 是 F 的一个子域．如同在 §3.2 中，我们可构造 F 的如下子集：

$$A(E, \leqslant) = \{a \in F \mid 有\ e \in E, 使得\ -e \leqslant a \leqslant e\}.$$

显然， $A(E, \leqslant)$ 关于 $\leqslant$ 是凸的，且 $E \subseteq A(E, \leqslant)$. 实际上，可建立如下结论.

引理 5.7.2 所设同上，则 $A(E,\leqslant)$ 是 F 的一个关于 $\leqslant$ 凸的赋值环.

证明 显然，$A(E,\leqslant)$ 对于加法与减法都是封闭的. 设 $a, b\in A(E,\leqslant)$, 则有 $e_1, e_2\in E$, 使得 $-e_1\leqslant a\leqslant e_1$ 且 $-e_2\leqslant b\leqslant e_2$. 不妨设 $a>0$ 且 $b>0$. 此时有 $0<a\leqslant e_1<1+e_1^2$, 且 $0<b\leqslant e_2<1+e_2^2$. 由命题 5.5.3(6) 知，$0<a^2<(1+e_1^2)^2$, 且 $0<b^2<(1+e_2^2)^2$. 由此有 $\pm ab\leqslant \dfrac{a^2+b^2}{2}<\dfrac{1}{2}[(1+e_1^2)^2+(1+e_2^2)^2]$, 其中 $\dfrac{1}{2}[(1+e_1^2)^2+(1+e_2^2)^2]\in E$. 从而可知 $ab\in A(E,\leqslant)$. 因而 $A(E,\leqslant)$ 是 F 的一个子环.

设 $a\in F$, 但 $a\notin A(E,\leqslant)$. 不失一般性，可进一步设 $0<a$. 此时必有 $1<a$. 由命题 5.5.3 知，$0<a^{-1}<1$. 从而 $a^{-1}\in A(E,\leqslant)$. 因此，$A(E\leqslant)$ 是 F 的一个赋值环. 证毕.

定理 5.7.3 设 $\leqslant$ 是域 F 的一个半序，A 是 F 的一个子集，则 A 是 F 的一个关于 $\leqslant$ 凸的赋值环，当且仅当 $A=A(E,\leqslant)$, 这里 E 是 F 的一个子域.

证明 充分性由引理 5.7.2 可推出，下证必要性.

由于 A 是关于 $\leqslant$ 凸的子环，从而易知，$\mathbb{Q}\subseteq A$. 由 Zorn 引理，A 包含 F 的一个极大子域 E. 显然，$A(E,\leqslant)\subseteq A$. 设 $\alpha\in A$, 则由定理 3.2.2 中蕴含关系 "(1) $\Longrightarrow$ (2)" 的证明可知，有如下关系式:

$$\alpha^n+a_1\alpha^{n-1}+\cdots+a_n=\eta\in M,$$

这里 M 是 A 的极大理想，$a_1,\cdots,a_n\in E$.

根据定理 5.5.7 的证明知，$-M<\alpha<M$, 其中 $M=\dfrac{1}{2}[n+1+a_1^2+\cdots+a_{n-1}^2+(a_n-\eta)^2]$. 假若 $\eta^2\geqslant 1$, 则有 $0<\eta^{-2}\leqslant 1\in A$. 由 A 关于 $\leqslant$ 的凸性知，$\eta^{-2}\in A$, 即 $\eta^{-1}\in A$, 矛盾. 从而 $\eta^2<1$. 由此有 $(a_n-\eta)^2=a_n^2-2a_n\eta+\eta^2\leqslant a_n^2+a_n^2+\eta^2+\eta^2<2a_n^2+2$. 于是 $-M_1<\alpha<M_1$, 这里 $M_1=\dfrac{1}{2}(n+3+a_1^2+\cdots+a_{n-1}^2+2a_n^2)\in E$. 由 $A(E,\leqslant)$ 的构造知，$\alpha\in A(E,\leqslant)$. 因此，$A=A(E,\leqslant)$. 证毕.

推论 1 域 F 有一个非阿基米德半序，当且仅当 F 有一个非阿基米德序.

证明 由于序总是半序，从而充分性成立. 现设 $\leqslant$ 是 F 的一个非阿基米德半序，则 $A(\mathbb{Q},\leqslant)$ 是 F 的一个实赋值环，且 $A(\mathbb{Q},\leqslant)\neq F$. 由定理 3.1.4 知，$A(\mathbb{Q},\leqslant)$ 的对应赋值 v 与 F 的某个序相容. 显然，这个序是非阿基米德的. 证毕.

推论 2 设 $\leqslant$ 是域 F 的一个半序，则 F 的所有关于 $\leqslant$ 凸的赋值环对于集合的包含关系组成一个链，且其中最小成员为 $A(\mathbb{Q},\leqslant)$.

证明 参见定理 3.2.2 的推论 3.

推论 3 设 P 是域 F 的一个半锥，E 是 F 的一个子域，且 M 是赋值环 $A:=A(E,\leqslant_P)$ 的极大理想，则 E 可看作剩余域 A/M 的一个子域，且如下子集

$$(P\cap A)+M/M:=\{a+M\mid a\in P\cap A\}$$

是剩余域 A/M 的一个在 E 上的阿基米德半锥.

证明　参见定理 3.2.2 的推论 2.

下面定理给出了一个域的不同实赋值之间某种联系.

定理 5.7.4　设 $\leqslant$ 是域 F 的一个半序，v_1, v_2 都是 F 的实赋值，则如下叙述成立：

(1) 若 $A_{v_1}\subseteq A_{v_2}$ 且 v_1 与 $\leqslant$ 相容，则 v_2 与 $\leqslant$ 相容；

(2) 若 $A_{v_1}\subseteq A_{v_2}$，则 $\mathcal{Y}_F^{v_1}\subseteq\mathcal{Y}_F^{v_2}$；

(3) 若 $\mathcal{Y}_F^{v_1}\cap\mathcal{Y}_F^{v_2}\neq\phi$，则 $\mathcal{Y}_F^{v_1}\subseteq\mathcal{Y}_F^{v_2}$ 或 $\mathcal{Y}_F^{v_2}\subseteq\mathcal{Y}_F^{v_1}$.

证明　(1) 设 $0<a\leqslant b$，则由 v_1 与 $\leqslant$ 的相容性知，$v_1(a)\geqslant v_1(b)$，即有 $ab^{-1}\in A_{v_1}\subseteq A_{v_2}$. 从而 $v_2(ab^{-1})\geqslant 0$，即 $v_2(a)\geqslant v_2(b)$. 由定义知，v_2 与 $\leqslant$ 相容.

(2) 由叙述 (1) 即得.

(3) 由条件知，有 $P\in\mathcal{Y}_F^{v_1}\cap\mathcal{Y}_F^{v_2}$. 从而 v_1 和 v_2 与半锥 P 都相容. 由命题 5.6.2 知，A_{v_1} 和 A_{v_2} 关于半序 $\leqslant_P$ 都是凸的. 再由定理 5.7.3 的推论 2 知，$A_{v_1}\subseteq A_{v_2}$ 或 $A_{v_2}\subseteq A_{v_1}$. 根据叙述 (2)，$\mathcal{Y}_F^{v_1}\subseteq\mathcal{Y}_F^{v_2}$ 或 $\mathcal{Y}_F^{v_2}\subseteq\mathcal{Y}_F^{v_1}$. 证毕.

由命题 3.2.3 知，域 F 的每个非阿基米德序必与某个非浅显的赋值相容. 自然会问：对于非阿基米德半序，相应的结论是否也成立？下面的例子表明，回答是否定的.

例　设 $F=\mathbb{Q}(x_1,x_2,\cdots,x_n,\cdots)$，其中 $x_1, x_2, \cdots, x_n, \cdots$ 是有理数域 $\mathbb{Q}$ 上可数个未定元. 在实数域 $\mathbb{R}$ 的开区间 $]0,1[$ 中任取可数个代数无关的超越元 $\alpha_1, \alpha_2, \cdots, \alpha_n, \cdots$，则有 F 到 $\mathbb{R}$ 的一个嵌入 π，使得 $\pi(x_i)=\alpha_i$，$i=1, 2, \cdots$. 令 $P'=\pi^{-1}(\mathbb{R}^2)$，则 P' 是 F 的一个正锥，使得 $x_i, 1-x_i\in P'$，$i=1,2,\cdots$.

记 $F_0=\mathbb{Q}$，且 $F_n=\mathbb{Q}(x_1,\cdots,x_n)$，$n=1, 2, \cdots$. 下面将归纳地规定 F_n 的一个半锥 P_n，使得对于每个自然数 n，$P_n\cap F_{n-1}=P_{n-1}$.

首先，令 P_0 是 F_0 的惟一正锥. 假定 F_n 的一个半锥 P_n 已经被规定，使得 $P_n\cap F_{n-1}=P_{n-1}$，且对于每个 $a\in F_{n-1}$，$x_n-a\in P_n$. 现考虑域 $F_{n+1}=F_n(x_{n+1})$. 由命题 3.1.1(2) 知，F_{n+1} 有一个赋值 v_n，使得对于非零多项式 $f(x_{n+1})\in F_n[x_{n+1}]$，$-v_n(f(x_{n+1}))$ 为 $f(x_{n+1})$ 的次数，v_n 的值群为 $\mathbb{Z}$，且剩余域可等同于 F_n. 显然 $v_n(x_{n+1})=-1$. 从而 v_n 有这样的一个截口 s: $\mathbb{Z}\longrightarrow F_{n+1}$，使得对于每个 $m\in\mathbb{Z}$，$s(m)=x_{n+1}^{-m}$.

令 σ: $\mathbb{Z}/2\mathbb{Z}\longrightarrow\{1,-1\}$ 是浅显的特征标，即对于每个 $\bar{m}\in\mathbb{Z}/2\mathbb{Z}$，$\sigma(\bar{m})=1$. 此外，令 $\mathcal{P}$ 是 $\mathbb{Z}/2\mathbb{Z}$ 到 $\mathcal{Y}_{F_n}$ 的这样一个映射，使得 $\mathcal{P}(\bar{0})=P_n$，而 $\mathcal{P}(\bar{1})=P'\cap F_n$. 由引理 5.6.5，$\mathcal{P}^\sigma$ 是 F_{n+1} 的一个与 v_n 相容的半锥. 从而令 $P_{n+1}=\mathcal{P}^\sigma$.

设 $a\in P_n$ 且 $a\neq 0$，则 $v_n(a)=0$ 且 $\dfrac{a}{s(v_n(a))}\sigma(\overline{v_n(a)})+M_{v_n}=a+M_{v_n}\equiv$

$a \in P_n = \mathcal{P}(\overline{v_n(a)})$. 从而 $a \in \mathcal{P}^\sigma = P_{n+1}$. 因而 $P_{n+1} \cap F_n = P_n$. 此外，对于每个 $a \in F_n$，由于 $\dfrac{x_{n+1}-a}{s(v_n(x_{n+1}-a))}\sigma(\overline{v_n(x_{n+1}-a)}) + M_{v_n} = \dfrac{x_{n+1}-a}{x_{n+1}} + M_{v_n} = 1 + M_{v_n} \in \mathcal{P}(\overline{v_n(x_{n+1}-a)})$，从而 $x_{n+1} - a \in P_{n+1}$. 类似地可推出，$x_n x_{n+1}$, $x_{n+1}(1-x_n) \in P_{n+1}$.

令 $P = \bigcup\limits_{n=1}^{\infty} P_n$，则 P 显然为 F 的一个半锥，使得 $x_n x_{n+1}, x_{n+1}(1-x_n) \in P$，且对于每个 $\alpha \in F_n$, $x_{n+1} - \alpha \in P$, $n = 1, 2, \cdots$. 由于 $x_{n+1}, x_n - 1 \in P$，但 $x_{n+1}(1-x_n) \in P$，从而 P 是一个真半锥，自然是非阿基米德的 (参见定理 5.5.6).

现假设 P 与 F 的某个非浅显赋值 v 相容，则由命题 5.6.2 知，v 的赋值环 A_v 关于 $\leqslant_P$ 是凸的. 由于 $A_v \neq F$，从而有某个 $\alpha \in F$，使得 $\alpha \notin A_v$. 于是对于某个自然数 n, $\alpha \in F_{n-1}$. 由于 $x_n \pm \alpha \in P_n$，从而 $-x_n <_P \alpha <_P x_n$. 由 A_v 关于 $\leqslant_P$ 的凸性知，$x_n \notin A_v$，即 $v(x_n) < 0$. 从而有 $v(x_n x_{n+1}) < v(x_{n+1})$. 然而，$0 <_P x_n x_{n+1} <_P x_{n+1}$，这矛盾于 v 与 P 的相容性. 因此，P 与 F 的每个非浅显赋值都不相容.

上面的例子也说明了这样一个重要事实：在命题 5.6.2 中，蕴含关系 “(2) $\Longrightarrow$ (1)” 在一般情况下是不成立的. 事实上，在上面例子中，令 v 是赋值环 $A(\mathbb{Q}, \leqslant_P)$ 所对应的赋值，则 v 是 F 的一个非浅显赋值. 由上面讨论，v 不与 $\leqslant_P$ 相容. 然而，由引理 5.7.2 知，$A(\mathbb{Q}, \leqslant_P)$ 关于 $\leqslant_P$ 是凸的. 很自然，命题 5.6.2 中蕴含关系 “(4) $\Longrightarrow$ (1)” 在一般情况下也是不成立的.

现在，我们考虑半序与 Hensel 赋值之间的关系. 作为定理 3.4.5 对半序的推广，我们可建立下面结论.

定理 5.7.5 设 (F, v) 是一个 Hensel 赋值域，则 $\mathcal{Y}_F^v = \mathcal{Y}_F$，即 v 与 F 的每个半序相容.

证明 设 $\leqslant$ 是 F 的任意半序，且 $0 < c \leqslant d$，其中 $c, d \in F$. 假若 $v(c) < v(d)$，则 $b = dc^{-1} \in M_v$，这里 M_v 是 v 的赋值理想. 根据定理 3.4.5 的类似论证，有 $b = -a^2 - a$，其中 $a \in F$. 由此有 $d = c(-a^2 - a) = c - c\left(a + \dfrac{1}{2}\right)^2 - \dfrac{3}{4}c < c$，矛盾. 因而 $v(c) \geqslant v(d)$. 证毕.

将上面定理与定理 5.6.7 的推论 2 结合起来，可以得到满足 WH 的 Hensel 域的如下一个刻画.

定理 5.7.6 设 v 是域 F 的一个 Hensel 赋值，则 $\mathcal{X}_F = \mathcal{Y}_F$，当且仅当 $|G_v/2G_v| = 2$ 与 $|\mathcal{X}_{F_v}| = 1$，或者 $|G_v/2G_v| = 1$ 与 $\mathcal{X}_{F_v} = \mathcal{Y}_{F_v}$.

为举例说明定理 5.7.6，我们给出下面的例子.

例 2 设 F 是一个域，$(G, \leqslant)$ 是一个运算为加法 $+$ 的序群，记 F^G 为集合 G 到 F 的全体映射组成的集合. 对于 $f \in F^G$，可规定 G 的如下子集：

$$\text{supp}(f) = \{g \in G \mid f(g) \neq 0\}.$$

同时，称 $\text{supp}(f)$ 为 f 的支集．于是，可进一步得到 F^G 的如下子集：

$$F((G)) := \{f \in F^G \mid \text{supp}(f) = \phi \text{ 或 } \text{supp}(f) \text{ 对于 } \leqslant \text{ 是 } G \text{ 的良序子集 }\}.$$

此外，在 $F((G))$ 上按如下方式规定运算 "+" 和 "·"：对于 $f, h \in F((G))$ 以及 $g \in G$,

$$(f+h)(g) = f(g) + h(g);$$
$$(f \cdot h)(g) = \sum_{g_1+g_2=g} f(g_1)h(g_2).$$

容易证明 $F((G))$ 对于上面所规定的运算构成一个域．对于 $a \in F$, 用 $\hat{a}$ 表示 F^G 中这样的常量映射，使得对于每个 $g \in G$, $\hat{a}(g) = a$. 显然，$\hat{a} \in F((G))$. 易见，映射：$a \mapsto \hat{a}$ $(a \in F)$ 是域 F 到 $F((G))$ 的一个嵌入．将 a 和 $\hat{a}$ 等同，则可认定：$F \subseteq F((G))$. 这样所得的域 $F((G))$ 称作系数在 F 中而指数在 G 中的形式幂级数域．

对于非零 $f \in F((G))$, $\text{supp}(f) \neq \phi$. 从而可规定 $v(f)$ 是支集 $\text{supp}(f)$ 中最小元素．此外，规定 $v(0) = \infty$. 易见，v 是域 $F((G))$ 的一个赋值，它的值群为 G. 设 A_v 是 v 的赋值环，则可构造 A_v 到 F 的一个映射 ϕ, 使得对于每个 $f \in A_v$, $\phi(f) = f(0)$. 易知，ϕ 是环之间的一个满同态，且同态核 $\ker\phi$ 恰为 v 的赋值理想 M_v. 由环同态基本定理，剩余域 $F_v = A_v/M_v \cong F$. 该赋值 v 称作域 $F((G))$ 的自然赋值．

作为赋值论中一个重要事例，$(F((G)), v)$ 是一个 Hensel 赋值域．

根据上面的定理 5.7.6, 域 $\mathbb{R}((\mathbb{Z}))$, $\mathbb{Q}((\mathbb{Z}))$ 都满足 WH. 此外，若 G 是 2- 可除的，即 $G = 2G$, 则域 $\mathbb{Q}((\mathbb{Z}))((G))$ 也满足 WH. 然而，域 $\mathbb{Q}(\sqrt{2})((\mathbb{Z}))$ 不满足 WH, 因为 $\mathbb{Q}(\sqrt{2})$ 有两个不同的序．

§5.8 关于弱迷向性的局部 – 整体原理

在本节中，我们将借助于域的实赋值以及它们的 Hensel 化，来研究域上二次型的弱迷向性．本节中一个主要结果 (定理 5.8.3) 原是由 L. Bröcker 提出的一个猜测，并在后来被 L. Bröcker 与 A. Prestel 各自独立地证实．

设 v 是域 F 的一个值群为 G 的赋值，且 s 是 v 的一个半截口．在集合 $\dot{F}$ 上可规定如下二元关系 $\sim_G$: $a \sim_G b$, 当且仅当 $v(a) - v(b) \in 2G$. 显然，$\sim_G$ 是集合 $\dot{F}$ 上一个等价关系．对于 F 上一个正则型 $q = \langle a_1, \cdots, a_n \rangle$, 通过调整元素 $a_1, \cdots, a_n$ 的位置，可使 $q \approx_F q_1 \oplus \cdots \oplus q_m$, 其中 $q_i = \langle a_{i1}, \cdots, a_{in_i} \rangle$ 中任意两个元素关于 $\sim_G$

都是等价的，而当 $i \neq j$ 时，q_i 和 q_j 中元素各属于关于 $\sim_G$ 的不同等价类.

注意到，对于每个 $a \in \dot{F}$, $as(v(a))^{-1} \in A_v \setminus M_v$. 从而 $\overline{a_{ij_i}s(v(a_{ij_i}))^{-1}} = a_{ij_i}s(v(a_{ij_i}))^{-1} + M_v$ 是 v 的剩余域 F_v 中非零元，$i = 1, \cdots, m; j_i = 1, \cdots, n_i$. 对于 $i = 1, \cdots, m$, 可构造域 F_v 上的如下正则型：

$$q_i^v = \langle \overline{a_{i1}s(v(a_{i1}))^{-1}}, \cdots, \overline{a_{in_i}s(v(a_{in_i}))^{-1}} \rangle,$$

且称它们为 q 关于 v 的剩余类型.

定理 5.8.1 设 v 是域 F 的一个赋值，使得剩余域 F_v 的特征不为 2, 且 $q = q_1 \oplus \cdots \oplus q_m$ 是 F 上正则型，使得 $q_1^v, \cdots, q_m^v$ 为 q 关于 v 的剩余类型.

(1) 若 q 在 F 上迷向，则某个 q_i^v 在 F_v 上迷向.

(2) 若某个 q_i^v 在 F_v 上迷向，且 v 是 F 的 Hensel 赋值，则 q 在 F 上是迷向的.

证明 (1) 设 $q = \langle a_1, \cdots, a_n \rangle$, 其中 $a_r \in \dot{F}$, $r = 1, \cdots, n$, 则 F 中有不全为零的元素 $b_1, \cdots, b_n$, 使得 $\sum_{r=1}^{n} a_r b_r^2 = 0$. 令 $v(a_k b_k^2) = \min\{v(a_r b_r^2) \mid r = 1, \cdots, n\}$, $1 \leqslant k \leqslant n$, 则 $a_k b_k^2 \neq 0$. 不妨设 a_k 在型 q_1 中出现. 此时有 $\sum_{r=1}^{n} a_r s(v(a_k))^{-1}(b_r b_k^{-1})^2 = 0$. 设 $q_i = \langle a_{i1}, \cdots, a_{in_i} \rangle$, $i = 1, \cdots, m$, 则当 $i \neq 1$ 时，$v(a_{ij}b_{ij}^2) \neq v(a_k b_k^2)$; 否则 $v(a_{ij}) - v(a_k) \in 2G$, 即 $a_{ij} \sim_G a_k$. 从而必有 $v(a_{ij}b_{ij}^2) > v(a_k b_k^2) = v(s(v(a_k))b_k^2)$, 即 $\overline{a_{ij}s(v(a_k))^{-1}(b_{ij}b_k^{-1})^2} = \bar{0}$. 于是 $\sum_{j=1}^{n_1} \overline{a_{1j}s(v(a_k))^{-1}(b_{1j}b_k^{-1})^2} = \overline{\sum_{r=1}^{n} a_r s(v(a_k))^{-1}(b_r b_k^{-1})^2} = \bar{0}$. 由于 $v(a_{1j}) - v(a_k) \in 2G$, 从而有 $\xi_j \in \dot{F}$, 使得 $s(v(a_{1j})) = s(v(a_k))\xi_j^2$, $j = 1, \cdots, n_1$. 于是 $a_{1j}s(v(a_k))^{-1}\ (b_{1j}b_k^{-1})^2 = a_{1j}s(v(a_{1j}))^{-1}(b_{1j}\xi_j b_k^{-1})^2$, $j = 1, \cdots, n_1$. 显然 $b_{1j}\xi_j b_k^{-1} \in A_v$, $j = 1, \cdots, n_1$. 从而有 $\sum_{j=1}^{n_1} \overline{a_{1j}s(v(a_{1j}))^{-1}}(\overline{b_{1j}\xi_j b_k^{-1}})^2 = \bar{0}$. 这表明：$q_1^v$ 在 F_v 上是迷向的.

(2) 令 $q_i = \langle a_{i1}, \cdots, a_{in_i} \rangle$, $i = 1, \cdots, m$. 不妨设 q_1^v 在 F_v 上是迷向的，则有 $b_1, \cdots, b_{n_1} \in A_v$, 使得 $\sum_{j=1}^{n_1} a_{1j}s(v(a_{1j}))^{-1}b_j^2 \in M_v$, 但 $b_1, \cdots, b_{n_1}$ 不全属于 M_v. 不妨设 $b_1 \notin M_v$. 考察二次多项式 $f(x) = a_{11}s(v(a_{11}))^{-1}x^2 + \sum_{j=2}^{n_1} a_{1j}s(v(a_{1j}))^{-1}b_j^2 \in A_v[x]$. 显然有

$$\begin{aligned} f(x) &\equiv a_{11}s(v(a_{11}))^{-1}x^2 - a_{11}s(v(a_{11}))^{-1}b_1^2 \\ &\equiv a_{11}s(v(a_{11}))^{-1}(x + b_1)(x - b_1) \pmod{M_v}. \end{aligned}$$

注意到 F_v 的特征 $\neq 2$, 从而 $F_v[x]$ 中多项式 $x+\bar{b}_1$ 和 $x-\bar{b}_1$ 是互素的. 由 Hensel 引理知, $f(x)$ 在 A_v 中有根 d, 使得 $\bar{d}=\bar{b}_1$. 此外, 由上面讨论知, 有 $\xi_j \in \dot{F}$, 使得 $s(v(a_{1j}))=s(v(a_{11}))\xi_j^2, j=1,\cdots,n_1$. 于是有 $s(v(a_{11}))^{-1}\left[a_{11}d^2+\sum_{j=2}^{n_1}a_{1j}(b_j\xi_j^{-1})^2\right]=f(d)=0$, 即 $a_{11}d^2+\sum_{j=2}^{n_1}a_{1j}(b_j\xi_j^{-1})^2=0$. 因而 q_1 在 F 上迷向, 必然 q 在 F 上迷向. 证毕.

注　若在上面定理的叙述 (2) 中, 不假定 v 是 Hensel 赋值, 则由上面的论证仅能得到

$$\min\{v(a_{1j}s(v(a_{1j}))^{-1}b_j^2)\mid j=1,\cdots,n_1\}=0<v\left(\sum_{j=1}^{n_1}a_{1j}s(v(a_{1j}))^{-1}b_j^2\right)\in G_v.$$

由此可知, 存在不全为零的 $c_1,\cdots,c_n\in F$, 使得

$$\min\{v(a_jc_j^2)\mid j=1,\cdots,n\}<v\left(\sum_{j=1}^{n}a_jc_j^2\right)\in G_v.$$

定理 5.8.1 表明, 关于 Hensel 赋值域上二次型的迷向性的讨论可归结于剩余域上的相同问题. 为了借助于实赋值讨论二次型的弱迷向性, 我们还需要反映半序和实赋值之间联系的更进一步结果.

命题 5.8.2　设 v 是域 F 的一个赋值, $\leqslant$ 是 F 的一个半序, 使得 v 的赋值环 A_v 关于 $\leqslant$ 是凸的. 如果对于 $a,b\in F$ 以及 $g\in G_v$, $0<a$, $v(a)\leqslant 2g\leqslant v(b)$ 且 $v(a)\neq v(b)$, 那么 $b<a$.

证明　令 $g=v(c)$, 其中 $c\in\dot{F}$, 且不妨设 $0<b$. 由 $v(a)\leqslant v(c^2)\leqslant v(b)$ 知, $v(ac^{-2})\leqslant 0\leqslant v(bc^{-2})$. 由于 $v(a)\neq v(b)$, 从而有如下两种可能情形:

情形 1　$v(ac^{-2})<0\leqslant v(bc^{-2})$. 此时 $bc^{-2}\in A_v$, 但 $ac^{-2}\notin A_v$. 由于 $ac^{-2}>0$, 从而由 A_v 关于 $\leqslant$ 的凸性知, $bc^{-2}<ac^{-2}$, 即 $b<a$.

情形 2　$v(ac^{-2})\leqslant 0<v(bc^{-2})$. 此时 $bc^{-2}\in M_v$, 但 $ac^{-2}\notin M_v$. 由命题 5.6.2 知, M_v 关于 $\leqslant$ 是凸的. 由此也有 $bc^{-2}<ac^{-2}$, 即 $b<a$. 证毕.

推论　设 v 是域 F 的一个赋值, $\leqslant$ 是 F 的一个半序, 使得 A_v 关于 $\leqslant$ 是凸的. 如果对于任意 $g_1,g_2\in G_v$, 其中 $g_1<g_2$, 存在 $g\in G_v$, 使得 $g_1\leqslant 2g\leqslant g_2$, 则 v 与 $\leqslant$ 相容. 特别地, 当 G_v 是 2- 可除的或 $G_v\cong\mathbb{Z}$ 时, v 与 $\leqslant$ 相容.

证明　根据定义 5.6.2, 由命题 5.8.2 即得结论.

下面给出一种适合弱迷向正则型的局部 - 整体原理，它是通过域的序以及实赋值的 Hensel 化来表达的.

定理 5.8.3 设 q 是实域 F 上一个正则型. 若 q 对于 F 的每个序都是不定的, 且 q 在 F 的所有使得 $G_v \neq 2G_v$ 的实赋值 v 的 Hensel 化上是弱迷向的, 则 q 在 F 上是弱迷向的.

证明 不妨设 $q = \langle a_1, \cdots, a_n \rangle$, 且假设 q 在 F 上不是弱迷向的. 由定理 5.5.11 知, F 有一个半锥 P, 使得 q 关于 P 是正定或负定的. 不失一般性, 设 q 关于 P 是正定的. 由所设, P 是 F 的一个真半锥, 从而是非阿基米德的. 由引理 5.7.2, $A(\mathbb{Q}, \leqslant_P)$ 是 F 的一个关于 $\leqslant_P$ 凸的赋值环, 且 $A(\mathbb{Q}, \leqslant_P) \neq F$. 令 v 是赋值环 $A(\mathbb{Q}, \leqslant_P)$ 所对应的赋值, 则由命题 5.7.1 知, v 是 F 的一个实赋值.

假设 $v(a_i) \in 2G_v$, $i = 1, \cdots, n$, 则有 $b_i \in \dot{F}$, 使得 $v(a_i) = 2v(b_i)$, $i = 1, \cdots, n$. 此时, $q \approx_F \langle a_1 b_1^{-2}, \cdots, a_n b_n^{-2} \rangle$, 且 $a_i b_i^{-2} \in A_v \setminus M_v$, $i = 1, \cdots, n$. 从而不妨直接设 $a_i \in A_v \setminus M_v$, $i = 1, \cdots, n$. 由定理 5.7.3 的推论 3 和定理 5.5.6 可知, $(P \cap A_v) + M_v/M_v$ 是剩余域 F_v 的一个 (阿基米德) 序. 由 Baer-Krull 定理 (定理 5.6.7 的推论 1) 知, F 有一个正锥 P_1, 使得 v 与 P_1 相容, 且 P_1 在 F_v 上所诱导的正锥恰为 $(P \cap A_v) + M_v/M_v$. 此时有 $a_i \in P_1$, $i = 1, \cdots, n$. 于是, q 对于 F 的正锥 P_1 是正定的, 与所设矛盾. 因而 $v(a_1), \cdots, v(a_n)$ 不都属于 $2G_v$. 自然, G_v 不是 2- 可除的.

显然, 陪集 $v(a_i) + 2G_v$ 中必有大于或等于零的元素 (即非负元素), $i = 1, \cdots, n$. 对于 $i = 1, \cdots, n$, 记 G_i 是由 G_v 中所有这样的元素 g 组成的集合, 使得对于任意自然数 k 以及 $v(a_i) + 2G_v$ 中任意非负元素 $v(a_i) + 2g_1$, $-v(a_i) - 2g_1 \leqslant kg \leqslant v(a_i) + 2g_1$. 显然, G_i 是序群 G_v 的凸子群, $i = 1, \cdots, n$. 注意到, 序群的全部凸子群对于集合的包含关系组成一个链. 从而, 不妨设 $G_i \subseteq G_1$, $i = 2, \cdots, n$. 考虑商群 $\overline{G} = G_v/G_1$, 则 G_v 的序 $\leqslant$ 诱导出 $\overline{G}$ 的一个序 $\preceq$, 使得 $g_1 + G_1 \prec g_2 + G_1$, 当且仅当 $g_1 < g_2$ 且 $g_1 - g_2 \notin G_1$. 同时, 可规定 F 的一个赋值 v_1, 使得对于每个 $a \in \dot{F}$, $v_1(a) = v(a) + G_1$. 此时易知, $A_v \subseteq A_{v_1}$. 由定理 5.7.4 知, $\mathcal{Y}_F^v \subseteq \mathcal{Y}_F^{v_1}$. 由于 v 是一个实赋值, 从而 $\mathcal{Y}_F^v \neq \phi$, 即有 $\mathcal{Y}_F^{v_1} \neq \phi$. 这表明 v_1 是 F 的一个实赋值. 显然, v_1 的值群为 $\overline{G}$. 此外, 可断定: $\overline{G}$ 不是 2- 可除的. 事实上, 如若不然, 则有某个 $g_1 \in G_v$, 使得 $v(a_1) - 2g_1 \in G_1$. 令 $h = \max\{v(a_1) - 2g_1, 2g_1 - v(a_1)\}$, 则有 $h \in G_1$, 且 $0 \leqslant h$. 注意到 $h - v(a_1) \in 2G_v$, 从而 h 是 $v(a_1) + 2G_v$ 中非负元素. 由 G_1 的构造知, $2h \leqslant h$, 即 $h \leqslant 0$. 从而 $h = 0$. 于是, $v(a_1) = 2g_1$, 即有 $v(a_1) + 2G_v = 2G_v$. 此时易知, $G_1 = \{0\}$. 从而 $\overline{G} \cong G_v$, 这矛盾于事实 G_v 不是 2- 可除的.

由所设知, 对于某个自然数 m, 型 $m \times q$ 在 v_1 的 Hensel 化上是迷向的. 记 $m \times q = \langle d_1, \cdots, d_{mn} \rangle$. 注意到 v_1 的 Hensel 化的剩余域等同于 F_{v_1}. 从而由定理 5.8.1 后的注知, 有不全为零的 $c_1, \cdots, c_{mn} \in F$, 使得

$$\min\{v_1(d_i c_i^2) \mid i = 1, \cdots, mn\} \prec v_1\left(\sum_{i=1}^{mn} d_i c_i^2\right), \text{且 } v_1\left(\sum_{i=1}^{mn} d_i c_i^2\right) \in \overline{G}.$$

令 $v_1(d_kc_k^2) = \min\{v_1(d_ic_i^2) \mid i = 1, \cdots, mn\}, 1 \leqslant k \leqslant mn$, 则 $d_kc_k^2 \neq 0$. 由上式有

$$v_1(d_k) \prec v_1\left(d_k + \sum_{i \neq k} d_i(c_ic_k^{-1})^2\right).$$

注意到 $d_k \in \{a_1, \cdots, a_n\}$, 从而 $d_k = a_j$, $1 \leqslant j \leqslant n$. 此时有

$$v_1(a_j) \prec v_1(a_j + p),$$

这里 $p = \sum_{i \neq k} d_i(c_ic_k^{-1})^2 \in P$.

由此有 $v(a_j) < v(a_j + p)$, 且 $g_0 := v(a_j + p) - v(a_j) \notin G_1$. 自然 $g_0 \notin G_j$. 由凸子群 G_j 的构造知，有某个自然数 r 以及某个 $g_1 \in G_v$, 使得

$$0 \leqslant v(a_j) + 2g_1 < rg_0.$$

选取 r 是满足上式的最小自然数，则有

$$(r-1)g_0 \leqslant v(a_j) + 2g_1 < rg_0.$$

当 r 为偶数时， $v(a_j + p) = g_0 + v(a_j) \geqslant g_0 + (r-1)g_0 - 2g_1 = rg_0 - 2g_1$, 而 $v(a_j) < rg_0 - 2g_1$, 其中 $rg_0 - 2g_1 \in 2G_v$; 当 r 为奇数时， $v(a_j + p) = g_0 + v(a_j) = (1-r)g_0 + v(a_j) + rg_0 > (1-r)g_0 + 2v(a_j) + 2g_1$, 而 $v(a_j) \leqslant v(a_j) + (v(a_j) + 2g_1 - (r-1)g_0) = (1-r)g_0 + 2v(a_j) + 2g_1$, 其中 $(1-r)g_0 + 2v(a_j) + 2g_1 \in 2G_v$. 因此，总有 $g \in G_v$, 使得 $v(a_j) \leqslant 2g \leqslant v(a_j + p)$. 根据命题 5.8.2, $a_j \geqslant a_j + p$. 从而 $-p = a_j - (a_j + p) \in P$, 必有 $p = 0$, 矛盾.

因此， q 在域 F 上是弱迷向的. 证毕.

由定理 5.8.3, 可以推导出如下简便的局部 - 整体原理.

定理 5.8.4 设 q 是实域 F 上一个正则型. 若 q 关于 F 的每个阿基米德序都是不定的，且 q 在 F 的每个非浅显实赋值的 Hensel 化上是弱迷向的，则 q 在 F 上是弱迷向的.

证明 由定理 5.8.3 知，只须证明： q 关于 F 的每个非阿基米德序是不定的. 设 P 是 F 的任意一个非阿基米德正锥. 由命题 3.2.3 知， F 有一个非浅显的实赋值 v, 使得 v 与 P 相容. 令 (K, w) 是赋值域 (F, v) 的 Hensel 化. 由所设知， q 在 K 上是弱迷向的. 由定理 3.4.6 知， P 可拓展为域 K 的一个正锥 Q. 显然， q 关于 Q 是不定的. 从而 q 关于 P 也是不定的. 证毕.

由 §5.7 中例 1 可见，对于一个实域 F, F 的所有阿基米德序以及所有与某个非浅显实赋值相容的半序不可能覆盖半序空间 $\mathcal{Y}_F$. 然而，应用上面的局部 - 整体

原理，可以证明下面的定理.

定理 5.8.5 设 F 是一个实域，则 F 的所有阿基米德序以及所有与某个非浅显实赋值相容的半序组成半序空间 $\mathcal{Y}_F$ 的一个稠密子集.

证明 设 $H_Y(a_1)\cap\cdots\cap H_Y(a_n)$ 是 $\mathcal{Y}_F$ 的任意一个非空的基本开集，其中 $a_1,\cdots,a_n\in\dot{F}$. 任取 $P_1\in H_Y(a_1)\cap\cdots\cap H_Y(a_n)$, 则型 $q=\langle 1,a_1,\cdots,a_n\rangle$ 关于 P_1 是正定的. 从而 q 在 F 上不是弱迷向的. 由定理 5.8.4 知， q 关于 F 的某个阿基米德序 P 是正定或负定的，或者 q 在 F 的某个非浅显实赋值 v 的 Hensel 化 (K,w) 上不是弱迷向的. 当 q 关于 P 是正定或负定时，由于 $1\in P$, 从而 $a_1,\cdots,a_n\in P$. 因而 $P\in H_Y(a_1)\cap\cdots\cap H_Y(a_n)$. 若 q 在 (K,w) 上不是弱迷向的，则由定理 5.5.11 知， q 对于 K 的某个半锥 Q 是正定或负定的. 由于 $1\in Q$, 从而必有 $a_1,\cdots,a_n\in Q$. 由定理 5.7.5 知，赋值 w 与 Q 相容. 于是， $v=w\,|_F$ 与 $Q\cap F$ 相容，且 $Q\cap F\in H_Y(a_1)\cap\cdots\cap H_Y(a_n)$. 证毕.

§5.9 Witt 环

在本节中，我们将针对特征不为 2 的域引进一个与二次型密切相关的交换环——Witt 环，同时研究实域的序与该域的 Witt 环的极小素理想之间的联系. 关于 Witt 环的研究是二次型理论中一个主要的组成部分，本节所介绍的有关内容仅限于本书的需要.

定义 5.9.1 域 F 上一个 $2n$ 维型 q 称作是双曲的，若 $q\approx_F n\times\langle 1,-1\rangle$. 一个 2 维的双曲型有时称作双曲面.

定理 5.9.1 域 F 上每个二次型 q 都有如下分解式:

$$q\approx_F s\times\langle 0\rangle\oplus m\times\langle 1,-1\rangle\oplus q_a,$$

其中 s,m 为非负整数， q_a 是 F 上一个反迷向型. 此外，非负整数 s,m 以及 q_a 的合同类是由 q 惟一确定的.

证明 由命题 5.1.1 可知， $q\approx_F s\times\langle 0\rangle\oplus q_1$, 其中 q_1 是 F 上一个正则型, s 是一个非负整数. 显然， $s=\dim(q)-\operatorname{rank}(q)$ 是由型 q 惟一确定的. 注意到, $q_1=0\times\langle 1,-1\rangle\oplus q_1$. 从而有一个最大非负整数 m, 使得 $q_1\approx_F m\times\langle 1,-1\rangle\oplus q_a$, 其中 q_a 是 F 上一个正则型. 假若 q_a 在 F 上是迷向的，则由命题 5.1.3 知， $q_a\approx_F\langle 1,-1\rangle\oplus\varrho$, 其中 ϱ 是 F 上一个正则型. 此时有 $q_1\approx_F(m+1)\times\langle 1,-1\rangle\oplus\varrho$, 与 m 的最大性矛盾. 因而， q_a 在 F 上是反迷向的，且 $q\approx_F s\times\langle 0\rangle\oplus m\times\langle 1,-1\rangle\oplus q_a$.

又设 $q\approx_F s\times\langle 0\rangle\oplus m'\times\langle 1,-1\rangle\oplus q_a'$, 其中 m' 为非负整数, q_a' 是 F 上一个反迷向型. 假若 $m'\neq m$, 则不妨设 $m'<m$. 由 Witt 消去定理有, $(m-m')\times\langle 1,-1\rangle\oplus q_a\approx_F q_a'$, 其中左端是一个迷向型，而右端是一个反迷向型，矛盾. 因而 $m'=m$. 再由

Witt 消去定理有， $q_a \approx_F q'_a$. 证毕.

在定理 5.9.1 的分解式中，型 q_a 称作 q 的反迷向部分. 由上面定理知，型 q 的反迷向部分在合同的意义下是由 q 惟一决定的.

现在，在域 F 上的所有正则型之间引进一个新的等价关系 —— 相似. 设 q 和 ϱ 是域 F 上两个正则型. 若有两个自然数 m, n, 使得

$$m \times \langle 1, -1\rangle \oplus q \approx_F n \times \langle 1, -1\rangle \oplus \varrho,$$

则称 q 与 ϱ 在 F 上相似，且记作： $q \sim_F \varrho$.

易知，相似关系 $\sim_F$ 是 F 上正则型之间的一个等价关系. 由相似关系 $\sim_F$ 所确定的等价类称作相似类. 对于 F 上正则型 q, 用 $[q]$ 表示 q 所在的相似类.

命题 5.9.2 设 F 是一个域，则下列叙述成立：

(1) 对于 F 的正则型 q, $q \sim_F 0$, 这里 0 为 F 上零维型，当且仅当 q 是双曲的；

(2) 对于 F 的两个正则型 q, ϱ, $q \approx_F \varrho$, 当且仅当 $q \sim_F \varrho$, 且 $\dim(q) = \dim(\varrho)$;

(3) 对于 F 的每个正则型 q, $q \sim_F q_a$, 其中 q_a 为 q 的反迷向部分；

(4) 在合同的意义下，每个型的相似类仅含有惟一的反迷向型.

证明 根据定义，叙述 (1), (2) 和 (3) 显然成立. 对于任意一个相似类 $[q]$, 由叙述 (3) 知 $q_a \in [q]$. 设 ϱ 是 $[q]$ 中另一反迷向型，则 $\varrho \sim_F q_a$. 从而 $m \times \langle 1, -1\rangle \oplus \varrho \approx_F n \times \langle 1, -1\rangle \oplus q_a$, 其中 m, n 为自然数. 根据定理 5.9.1 中惟一性， $\varrho \approx_F q_a$. 证毕.

用 $W(F)$ 表示域 F 上正则二次型的所有相似类组成的集合. 借助于二次型的直和与张量积，可以在 $W(F)$ 上规定两个运算如下：对于 $[q], [\varrho] \in W(F)$, 其中 q, ϱ 是 F 上正则型，

$$[q] \oplus [\varrho] = [q \oplus \varrho],$$
$$[q] \otimes [\varrho] = [q \otimes \varrho].$$

为证明上面所规定的运算是合理的，我们需要如下简单事实.

引理 5.9.3 设 q 是一个双曲型，则对于 F 的每个正则型 ϱ, $q \otimes \varrho$ 和 $\varrho \otimes q$ 是双曲的.

证明 由命题 5.1.7 知，只须证明： $\varrho \otimes q$ 是双曲型. 由条件，设 $q \approx_F m \times \langle 1, -1\rangle$, 且 $\varrho \approx_F \langle a_1, \cdots, a_n\rangle$, 其中 $a_1, \cdots, a_n \in \dot{F}$. 由命题 5.7.1 有， $\varrho \otimes q \approx_F m \times (\varrho \otimes \langle 1, -1\rangle) = m \times (\langle a_1, -a_1\rangle \oplus \cdots \oplus \langle a_n, -a_n\rangle)$. 由命题 5.1.3 的推论有，$\varrho \otimes q \approx_F (mn) \times \langle 1, -1\rangle$. 证毕.

现在，我们来验证上面所规定的运算是合理的：

设 $[q] = [q_1]$, 且 $[\varrho] = [\varrho_1]$, 则 $q \sim_F q_1$, 且 $\varrho \sim_F \varrho_1$. 从而有 $q \oplus H_1 \approx_F q_1 \oplus H_2$ 且 $\varrho \oplus H_3 \approx_F \varrho_1 \oplus H_4$, 这里 H_i 是 F 上双曲型， $i = 1, 2, 3, 4$. 根据命题 5.1.7, 有下面关系式：

$$(q \oplus \varrho) \oplus (H_1 \oplus H_3) \approx_F (q_1 \oplus \varrho_1) \oplus (H_2 \oplus H_4),$$
$$(q \otimes \varrho) \oplus (q \otimes H_3 \oplus H_1 \otimes \varrho \oplus H_1 \otimes H_3) \approx_F (q_1 \otimes \varrho_1) \oplus (q_1 \otimes H_4 \oplus H_2 \otimes \varrho_1 \oplus H_2 \otimes H_4).$$

显然, $H_1 \oplus H_3$ 和 $H_2 \oplus H_4$ 都是双曲型. 此外, 由引理 5.9.3 知, $q \otimes H_3 \oplus H_1 \otimes \varrho \oplus H_1 \otimes H_3$ 与 $q_1 \otimes H_4 \oplus H_2 \otimes \varrho_1 \oplus H_2 \otimes H_4$ 也都是双曲型. 从而有 $[q \oplus \varrho] = [q_1 \oplus \varrho_1]$, 且 $[q \otimes \varrho] = [q_1 \otimes \varrho_1]$. 这表明上面所规定的运算是合理的.

命题 5.9.4 对于上面所规定的运算 $\oplus$ 与 $\otimes$, 集合 $W(F)$ 组成一个有单位元 $[\langle 1 \rangle]$ 的交换环.

证明 由命题 5.1.7 可知, $W(F)$ 对于 $\oplus$ 和 $\otimes$ 组成一个有单位元 $[\langle 1 \rangle]$ 的交换半环, 且它的零元为 $[0]$, 这里 0 是 F 上零维型. 此外由引理 5.9.3 知, 对于任意非零的 $[q] \in W(F)$, $q \oplus (\langle -1 \rangle \otimes q) \approx_F \langle 1, -1 \rangle \otimes q \sim_F 0$. 从而有 $[q] \oplus [\langle -1 \rangle \otimes q] = [\langle 1, -1 \rangle \otimes q] = [0]$. 因此, $W(F)$ 是一个交换环. 证毕.

定义 5.9.2 命题 5.9.4 中的交换环 $W(F)$ 称作域 F 的 Witt 环.

例 (1) 设 F 是代数闭域. 此时, $\dot{F} = \dot{F}^2$. 因而, 对于 F 上任意正则型 q, $q \approx_F \langle 1, 1, \cdots, 1 \rangle$. 注意到, $\langle 1, 1 \rangle \approx_F \langle 1, -1 \rangle$. 于是, 当 $\dim(q)$ 为偶数时, $q \sim_F 0$; 而当 $\dim(q)$ 为奇数时, $q \sim_F \langle 1 \rangle$. 从而 $[q] = [0]$ 或 $[\langle 1 \rangle]$, 即有 $W(F) = \{[0], [\langle 1 \rangle]\}$. 显然, 映射: $[q] \longmapsto \dim(q) + 2\mathbb{Z}$ 是 Witt 环 $W(F)$ 到剩余环 $\mathbb{Z}/2\mathbb{Z}$ 的一个同构.

(2) 设 R 是一个实闭域, 则 $R = R^2 \cup -R^2$. 此时, 对于 R 上任意正则型 q, $q \approx_F \langle 1, 1, \cdots, 1, -1, -1, \cdots, -1 \rangle$. 用 $\mathrm{sgn}(q)$ 表示型 q 关于正锥 R^2 的符号差. 显然, q 是双曲的, 当且仅当 $\mathrm{sgn}(q) = 0$. 从而易见, 映射: $[q] \longmapsto \mathrm{sgn}(q)$ 是 Witt 环 $W(R)$ 到整数环 $\mathbb{Z}$ 的一个同构.

设 $[q] \in W(F)$. 对于任意 $\varrho \in [q]$, 有 $\varrho \oplus H_1 \approx_F q \oplus H_2$, 其中 H_1 和 H_2 都是双曲型. 由此有 $\dim(\varrho) + 2\mathbb{Z} = \dim(q) + 2\mathbb{Z}$. 据此, 可得 $W(F)$ 到剩余域 $\mathbb{Z}/2\mathbb{Z}$ 的一个满同态 ϕ: $[q] \longmapsto \dim(q) + 2\mathbb{Z}$. 易知, 同态核为

$$I = \{[q] \mid \dim(q) \text{ 为偶数 }\}.$$

显然, I 是 $W(F)$ 的一个极大理想. 该理想 I 称作 Witt 环 $W(F)$ 的基本理想 .

命题 5.9.5 设 $\wp$ 是 $W(F)$ 的一个素理想, 则 $W(F)/\wp \cong \mathbb{Z}$ 或 $\mathbb{Z}/(p)$, 其中 p 为某个素数. $\wp$ 为 $W(F)$ 的基本理想, 当且仅当 $[\langle 1, 1 \rangle] \in \wp$.

证明 对于每个 $a \in \dot{F}$, $\langle 1, a \rangle \otimes \langle 1, -a \rangle \approx_F \langle 1, -a^2, a, -a \rangle = \langle 1, -a^2 \rangle \oplus \langle a, -a \rangle \approx_F \langle 1, -1 \rangle \oplus \langle 1, -1 \rangle \sim_F 0$. 从而有 $[\langle 1, a \rangle] \otimes [\langle 1, -a \rangle] = [0] \in \wp$. 由于 $\wp$ 是素理想, 从而 $[\langle 1, a \rangle] \in \wp$ 或 $[\langle 1, -a \rangle] \in \wp$. 由此有, $[\langle a \rangle] \equiv [\langle 1 \rangle] \pmod{\wp}$, 或者 $[\langle a \rangle] \equiv [\langle -1 \rangle] \pmod{\wp}$.

作 $\mathbb{Z}$ 到 $W(F)/\wp$ 的如下映射:

$$\phi:\quad n \longmapsto [n\times\langle 1\rangle]+\wp,\quad n\in\mathbb{Z}.$$

设 $[q]\in W(F)$, 且 $q\approx_F\langle a_1,\cdots,a_r\rangle$, 其中 $a_i\in\dot{F}$, $i=1,\cdots,r$. 由上面讨论知, $[q]=[\langle a_1,\cdots,a_r\rangle]\equiv[\langle\pm1,\pm1,\cdots,\pm1\rangle]\equiv[n\times\langle 1\rangle]\ (\mathrm{mod}\,\wp)$, 其中 n 为整数. 这表明: 映射 ϕ 是一个满射. 进一步可验证 ϕ 是一个环同态. 由环同态基本定理知, $W(F)/\wp\cong\mathbb{Z}/J$, 其中 J 是 ϕ 的同态核. 注意到, J 必为 $\mathbb{Z}$ 的素理想, 从而 $J=\{0\}$ 或 $J=(p)$, 其中 p 为某个素数. 因而 $W(F)/\wp\cong\mathbb{Z}$ 或 $\mathbb{Z}/(p)$.

设 I 为 $W(F)$ 的基本理想. 若 $\wp=I$, 则显然有 $[\langle 1,1\rangle]\in\wp$. 反过来, 设 $[\langle 1,1\rangle]\in\wp$, 则 $[\langle 1\rangle]\equiv[\langle -1\rangle]\ (\mathrm{mod}\,\wp)$. 由上面讨论知, 对于每个 $a\in\dot{F}$, $[\langle a\rangle]\equiv[\langle 1\rangle]\ (\mathrm{mod}\,\wp)$. 于是, 对于任意 $[q]\in I$, $n:=\dim(q)$ 为偶数. 从而 $[q]\equiv[n\times\langle 1\rangle]\equiv[0]\ (\mathrm{mod}\,\wp)$. 因而, $I\subseteq\wp$. 由 I 的极大性知, $\wp=I$. 证毕.

定理 5.9.6 若域 F 不是实域, 则基本理想 I 是 $W(F)$ 的惟一素理想.

证明 假设 $W(F)$ 有一个不同于 I 的素理想 $\wp$. 由命题 5.9.5 知, $[\langle 1,1\rangle]\notin\wp$. 考虑 $\dot{F}$ 的如下子集:

$$P=\{a\in\dot{F}\mid[\langle a\rangle]\equiv[\langle 1\rangle]\,(\mathrm{mod}\,\wp)\}.$$

显然, $P\cdot P\subseteq P$. 由命题 5.9.5 的证明知, $\dot{F}=P\cup -P$. 如若 $P\cap -P\neq\phi$, 则有 $a\in P\cap -P$. 从而 $[\langle a\rangle]\equiv[\langle 1\rangle]\equiv[\langle -a\rangle]\,(\mathrm{mod}\,\wp)$, 即有 $[\langle 1,1\rangle]\equiv[\langle a,-a\rangle]\equiv[0]\,(\mathrm{mod}\,\wp)$. 于是 $[\langle 1,1\rangle]\in\wp$, 矛盾. 因而, $P\cap -P=\phi$. 此外, 可断言 $P+P\subseteq P$. 事实上, 如若不然, 则有 $a,b\in P$, 使得 $a+b\notin P$. 此时 $a+b\neq 0$; 否则 $a\in P\cap -P$. 从而有 $a+b\in -P$. 由于 $a+b\in D_F(\langle a,b\rangle)$, 从而由命题 5.1.5 知, $\langle a,b\rangle\approx_F\langle a+b,(a+b)ab\rangle$. 显然, $(a+b)ab\in -P$. 从而有 $[\langle 1,1\rangle]\equiv[\langle a,b\rangle]=[\langle a+b,(a+b)ab\rangle]\equiv[\langle -1,-1\rangle]$ $(\mathrm{mod}\ \wp)$, 即有 $[\langle 1,1\rangle]\oplus[\langle 1,1\rangle]\equiv[\langle -1,-1\rangle]\oplus[\langle 1,1\rangle]\equiv[\langle -1,-1,1,1\rangle]\equiv[0]$ $(\mathrm{mod}\ \wp)$. 由此有, $[\langle 1,1\rangle]\otimes[\langle 1,1\rangle]=[\langle 1,1\rangle]\oplus[\langle 1,1\rangle]\in\wp$. 由 $\wp$ 的素性可得, $[\langle 1,1\rangle]\in\wp$, 矛盾. 这表明: $P+P\subseteq P$.

因此, $P\cup\{0\}$ 为域 F 的一个正锥, 矛盾于所设: F 不是实域. 证毕.

设 P 是域 F 的一个正锥, 即 $P\in\mathcal{X}_F$, 且 $[q]\in W(F)$. 对于任意 $\varrho\in[q]$, 有 $\varrho\oplus H_1\approx_F q\oplus H_2$, 其中 H_1 和 H_2 都是双曲型. 从而型 $\varrho\oplus H_1$ 和 $q\oplus H_2$ 关于正锥 P 具有相同的符号差, 即 $\mathrm{sgn}_P(\varrho\oplus H_1)=\mathrm{sgn}_P(q\oplus H_2)$. 注意到 $\mathrm{sgn}_P(H_1)=\mathrm{sgn}_P(H_2)=0$, 从而有 $\mathrm{sgn}_P(\varrho)=\mathrm{sgn}_P(q)$. 因而, 可规定 $W(F)$ 到 $\mathbb{Z}$ 的一个映射 sgn_P: $[q]\longmapsto\mathrm{sgn}_P(q)$, $[q]\in W(F)$. 显然, sgn_P 是一个环的满同态, 且同态核 $\ker(\mathrm{sgn}_P)$ 为 $W(F)$ 的一个素理想. 下面的定理表明, 这样所得的同态核恰好为 $W(F)$ 的全部极小素理想.

定理 5.9.7 设 F 是一个实域, 则存在一个从 $\mathcal{X}_F$ 到 $W(F)$ 的所有极小素理想的如下双射:

$$P \longmapsto \ker(\mathrm{sgn}_P), \quad P \in \mathcal{X}_F,$$

这里 sgn_P 表示由正锥 P 所确定的 $W(F)$ 到 $\mathbb{Z}$ 的满同态.

证明 设 $\wp$ 是 $W(F)$ 的任意极小素理想, 则必有 $\wp \neq I$, 这里 I 为 $W(F)$ 的基本理想. 由定理 5.9.6 的证明知, $P_\wp := \{a \in F \mid [\langle a\rangle] \equiv [\langle 1\rangle] \pmod{\wp}\} \cup \{0\}$ 是 F 的一个正锥. 显然, $\ker(\mathrm{sgn}_{P_\wp}) \subseteq \wp$. 由 $\wp$ 的极小性, $\wp = \ker(\mathrm{sgn}_{P_\wp})$. 这表明 $W(F)$ 的每个极小素理想都具有形式 $\ker(\mathrm{sgn}_P)$, $P \in \mathcal{X}_F$.

现证明: 对于每个 $P \in \mathcal{X}_F$, $\ker(\mathrm{sgn}_P)$ 必为 $W(F)$ 的极小素理想. 由于每个素理想必包含一个极小的素理想, 从而有 $W(F)$ 的一个极小素理想 $\wp$, 使得 $\wp \subseteq \ker(\mathrm{sgn}_P)$. 由前面的讨论知, $\wp = \ker(\mathrm{sgn}_{P_1})$, 其中 $P_1 \in \mathcal{X}_F$. 从而 $\ker(\mathrm{sgn}_{P_1}) \subseteq \ker(\mathrm{sgn}_P)$. 设 $a \in P_1$ 且 $a \neq 0$, 则 $\mathrm{sgn}_{P_1}(\langle -1, a\rangle) = 0$, 即 $[\langle -1, a\rangle] \in \ker(\mathrm{sgn}_{P_1}) \subseteq \ker(\mathrm{sgn}_P)$. 从而 $\mathrm{sgn}_P(\langle -1, a\rangle) = 0$. 这表明 $a \in P$. 因而 $P_1 \subseteq P$, 必然有 $P_1 = P$. 于是 $\ker(\mathrm{sgn}_P) = \wp$ 是 $W(F)$ 的极小素理想.

再设 $\ker(\mathrm{sgn}_{P_1}) = \ker(\mathrm{sgn}_{P_2})$, 其中 $P_1, P_2 \in \mathcal{X}_F$. 由刚才的论证知, $P_1 = P_2$. 因此, 上面定理成立.

设 F 是一个实域, 对于每个 $[q] \in W(F)$, 可规定 $\mathcal{X}_F$ 到 $\mathbb{Z}$ 的如下映射:

$$\mathrm{sgn}([q]): \quad P \longmapsto \mathrm{sgn}_P([q]) = \mathrm{sgn}_P(q), \quad P \in \mathcal{X}_F.$$

这样的一个映射 $\mathrm{sgn}([q])$ 称作 $[q]$ 的全符号差.

命题 5.9.8 全符号差 $\mathrm{sgn}([q])$ 是序空间 $\mathcal{X}_F$ 到 $\mathbb{Z}$ 的一个连续映射, 其中 $\mathbb{Z}$ 被赋予离散拓扑.

证明 不妨设 $q = \langle a_1, \cdots, a_n\rangle$, 其中 $a_1, \cdots, a_n \in \dot{F}$. 对于 $k \in \mathbb{Z}$, 若 $\dfrac{n+k}{2}$ 不是 0 到 n 之间的非负整数, 则显然 $\mathrm{sgn}([q])^{-1}(k) = \phi$; 若 $\dfrac{n+k}{2}$ 是 0 到 n 之间的一个整数 r, 则易知

$$\mathrm{sgn}([q])^{-1}(k) = \cup H(a_{i_1}, \cdots, a_{i_r}, -a_{i_{r+1}}, \cdots, -a_{i_n}),$$

这里 $i_1 \cdots i_r i_{r+1} \cdots i_n$ 取遍足标 $1, \cdots, n$ 的所有不同的排列. 证毕.

用 $C(\mathcal{X}_F, \mathbb{Z})$ 表示从 $\mathcal{X}_F$ 到 $\mathbb{Z}$ 的全部连续映射组成的集合. 对于 $f, g \in C(\mathcal{X}_F, \mathbb{Z})$, 可按如下方式规定它们的和与积:

$$f+g: \quad P \longmapsto f(P) + g(P),$$
$$fg: \quad P \longmapsto f(P) \cdot g(P).$$

对于任意 $k \in \mathbb{Z}$, 显然 $(f+g)^{-1}(k) = \bigcup\limits_{m \in \mathbb{Z}} (f^{-1}(m) \cap g^{-1}(k-m))$ 是 $\mathcal{X}_F$ 的一个开集. 从而 $f+g \in C(\mathcal{X}_F, \mathbb{Z})$. 当 $k \neq 0$ 时, $(fg)^{-1}(k) = \bigcup\limits_{m|k} (f^{-1}(m) \cap g^{-1}(km^{-1}))$

为 $\mathcal{X}_F$ 的开集；当 $k=0$ 时，$(fg)^{-1}(k)=f^{-1}(0)\cup g^{-1}(0)$ 为 $\mathcal{X}_F$ 的开集. 于是 $fg\in C(\mathcal{X}_F,\mathbb{Z})$. 因而由上面的规定，$C(\mathcal{X}_F,\mathbb{Z})$ 具有加法与乘法这两个运算. 通过常规的验证可知，对于所规定的运算，$C(\mathcal{X}_F,\mathbb{Z})$ 是一个有单位元的交换环，其零元为像恒为零的常量映射.

通过全符号差，我们可以得到环 $W(F)$ 到 $C(\mathcal{X}_F,\mathbb{Z})$ 的如下同态：

$$\mathrm{sgn}\colon\ [q]\longmapsto \mathrm{sgn}([q]),\quad [q]\in W(F).$$

显然，sgn 的同态核为

$$\ker(\mathrm{sgn})=\{[q]\mid \text{对于每个 } P\in\mathcal{X}_F,\ \mathrm{sgn}_P([q])=0\}=\bigcap_{P\in\mathcal{X}_F}\ker(\mathrm{sgn}_P).$$

由定理 5.9.7 知，$\ker(\mathrm{sgn})$ 恰为 $W(F)$ 的全体极小素理想的交，自然也等于 $W(F)$ 的全体素理想的交. 因而 $\ker(\mathrm{sgn})=\mathrm{Nil}(W(F))$. 这里 $\mathrm{Nil}(W(F))$ 为环 $W(F)$ 的诣零根 (即小根).

下面研究诣零根 $\mathrm{Nil}(W(F))$ 中元素 (即环 $W(F)$ 中幂零元) 的特征.

引理 5.9.9 设域 F 不为实域，则 $\mathrm{Nil}(W(F))=I$, 这里 I 为 $W(F)$ 的基本理想，且对于某个自然数 n, $2^nW(F)=\{[0]\}$.

证明 由定理 5.9.6 即知，$\mathrm{Nil}(W(F))=I$. 此时，$[\langle 1,1\rangle]\in I=\mathrm{Nil}(W(F))$. 因而有自然数 n, 使得 $[\langle 1,1\rangle]$ 的 n 次幂：$[\langle 1,1\rangle]\otimes\cdots\otimes[\langle 1,1\rangle]$ 等于 $[0]$, 即 $2^n[\langle 1\rangle]=[0]$. 由于 $[\langle 1\rangle]$ 为 $W(F)$ 中单位元，从而 $2^nW(F)=\{[0]\}$. 证毕.

引理 5.9.10 设 q 是域 F 上一个反迷向型，而在域 $F(\sqrt{d})$ 上是一个双曲型，其中 $d\in F$, 则 $q\approx_F\langle 1,-d\rangle\otimes\varrho$, 其中 ϱ 是 F 上一个型. 特别地，$q\approx_F -dq$.

证明 显然，$\sqrt{d}\notin F$. 不妨设 $q=\langle a_1,\cdots,a_n\rangle$, 其中 $a_i\in\dot{F}$, $i=1,\cdots,n$. 由于 q 在 $F(\sqrt{d})$ 上是双曲的，从而 q 在 $F(\sqrt{d})$ 上是迷向的. 因而有不全为零的元素 $\alpha_1,\cdots,\alpha_n\in F(\sqrt{d})$, 使得 $\sum\limits_{i=1}^n a_i\alpha_i^2=0$. 令 $\alpha_i=b_i+c_i\sqrt{d}$, 其中 $b_i, c_i\in F$, $i=1,\cdots,n$, 则 $b_1,\cdots,b_n$ 和 $c_1,\cdots,c_n$ 不全为零，且有

$$\sum_{i=1}^n a_i(b_i^2+dc_i^2)+2\sqrt{d}\sum_{i=1}^n a_ib_ic_i=0.$$

由此有 $\sum\limits_{i=1}^n a_i(b_i^2+dc_i^2)=0$, 且 $\sum\limits_{i=1}^n a_ib_ic_i=0$.

由于 q 在 F 上是反迷向的，从而由上面第一个等式知，$u_1=(b_1,\cdots,b_n)$ 和 $u_2=(c_1,\cdots,c_n)$ 都是 F 上非零 n 维行向量. 此外，可断言 $(a_1b_1,\cdots,a_nb_n)$ 和 $(a_1c_1,\cdots,a_nc_n)$ 在 F 上线性无关. 事实上，如若不然，则有非零元 $e\in F$, 使得

$a_ib_i = ea_ic_i$, 即 $b_i = ec_i$, $i = 1, \cdots, n$. 由上面第二个等式有 $e\sum_{i=1}^{n} a_ic_i^2 = 0$, 矛盾于 q 在 F 上的反迷向性.

考虑域 F 上如下线性方程组:

$$\begin{cases} a_1b_1x_1 + \cdots + a_nb_nx_n &= 0, \\ a_1c_1x_1 + \cdots + a_nc_nx_n &= 0. \end{cases}$$

由线性方程组理论, 上面方程组在 F^n 中有 $n-2$ 个线性无关的解 $u_3, \cdots, u_n$. 如若 u_2 可由 $u_3, \cdots, u_n$ 线性表出, 即 $u_2 = e_3u_3 + \cdots + e_nu_n$, 其中 $e_3, \cdots, e_n \in F$, 则 $\sum_{i=1}^{n} a_ic_i^2 = (a_1c_1, \cdots, a_nc_n)(e_3u_3^{\mathrm{T}} + \cdots + e_nu_n^{\mathrm{T}}) = 0$, 矛盾. 从而 $u_2, u_3, \cdots, u_n$ 在 F 上是线性无关的. 再如若 u_1 可由 $u_2, \cdots, u_n$ 线性表出, 即 $u_1 = e_2u_2 + \cdots + e_nu_n$, 其中 $e_2, \cdots, e_n \in F$, 则 $\sum_{i=1}^{n} a_ib_i^2 = (a_1b_1, \cdots, a_nb_n)(e_2u_2^{\mathrm{T}} + \cdots + e_nu_n^{\mathrm{T}}) = e_2\sum_{i=1}^{n} a_ib_ic_i = 0$, 矛盾. 因此, $u_1, \cdots, u_n$ 在 F 上线性无关.

令 $A = (u_1^{\mathrm{T}}, u_2^{\mathrm{T}}, \cdots, u_n^{\mathrm{T}})$, 则 A 是 F 上 n 级可逆矩阵. 由上面的事实可知,

$$A^t \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} A = \begin{pmatrix} d_1 & & \\ & d_2 & \\ & & B \end{pmatrix},$$

其中 $d_1 = \sum_{i=1}^{n} a_ib_i^2$, $d_2 = \sum_{i=1}^{n} a_ic_i^2$, 且 B 是 F 上一个 $n-2$ 级可逆矩阵. 由上面等式知 $d_1 = -dd_2$, 从而有 $q \approx_F \langle -dd_2, d_2\rangle \oplus q_1$, 这里 q_1 是矩阵为 B 的 $(n-2)$ 维型. 注意到 $\langle -dd_2, d_2\rangle \approx_{F(\sqrt{d})} \langle 1, -1\rangle$. 从而由所设可知, q_1 在 F 上是反迷向的, 而在 $F(\sqrt{d})$ 上是双曲的. 借助于归纳假定, 有 $q_1 \approx_F \langle 1, -d\rangle \otimes \varrho_1$, 这里 ϱ_1 是 F 上的一个型. 此时, $q \approx_F \langle 1, -d\rangle \otimes (\langle d_2\rangle \oplus \varrho_1)$. 因而, 引理中第一个断言是成立的.

此外, 由 $q \approx_F \langle 1, -d\rangle \otimes \varrho$ 可得, $-dq \approx_F \langle -d\rangle \otimes (\langle 1, -d\rangle \otimes \varrho) \approx_F \langle -d, d^2\rangle \otimes \varrho \approx_F \langle 1, -d\rangle \otimes \varrho \approx_F q$. 证毕.

定理 5.9.11(Pfister) 设 F 为实域, q 是 F 上一个正则型, 则下列叙述等价:

(1) $[q]$ 是 $W(F)$ 中幂零元;

(2) 对于每个 $P \in \mathcal{X}_F$, $\mathrm{sgn}_P(q) = 0$;

(3) q 在 F 的每个实闭包上是双曲的;

(4) 对于某个自然数 n, $2^n \times q \sim_F 0$;

(5) 对于某个自然数 m, $m \times q \sim_F 0$.

证明 "(1) $\Longleftrightarrow$ (2)" 来自于等式: $\mathrm{Nil}(W(F)) = \ker(\mathrm{sgn})$. 蕴含关系 "(2) $\Longleftrightarrow$ (3)" 以及 "(4) $\Longrightarrow$ (5) $\Longrightarrow$ (2)" 是显然的. 只剩下证明 "(1) $\Longrightarrow$ (4)".

设 $[q]$ 是 $W(F)$ 中幂零元. 假设对于每个自然数 n, $2^n \times q$ 与零维型 0 在 F 上不相似. 由 Zorn 引理可知, 在 F 的代数闭包中, 存在 F 的一个极大扩域 K, 使得对于每个自然数 n, $2^n \times q$ 与 0 在 K 上不相似. 由引理 5.9.9 知, K 是一个实域. 如若 $K = K^2 \cup -K^2$, 则易知 $q \sim_K s \times \langle 1 \rangle$, 其中 s 为整数. 注意到, K^2 是 K 的(惟一) 正锥, 从而 $P := K^2 \cap F$ 是 F 的一个正锥. 由叙述 (2) 知, $\mathrm{sgn}_P(q) = 0$. 由此有 $s = \mathrm{sgn}_{K^2}(s \times \langle 1 \rangle) = \mathrm{sgn}_{K^2}(q) = \mathrm{sgn}_P(q) = 0$. 这表明 $q \sim_F 0$, 矛盾. 因而, $K \neq K^2 \cup -K^2$, 即有 $a \in K$, 使得 $a \notin K^2 \cup -K^2$. 由 K 的极大性, 存在自然数 m, 使得 $2^m \times q \sim_{F(\sqrt{d})} 0$, 这里 $d = \pm a$.

令 $\varrho = 2^m \times q$, 且 ϱ^a 为它在 K 上的反迷向部分, 则 $\varrho^a \sim_{K(\sqrt{d})} \varrho \sim_{K(\sqrt{d})} 0$, 即 ϱ^a 在域 $K(\sqrt{d})$ 上是双曲的. 由引理 5.9.10, $\varrho^a \approx_K \langle -d \rangle \otimes \varrho^a$, 这里 $d = \pm a$. 此时, $2 \times \varrho \sim_K 2 \times \varrho^a \approx_K \langle a \rangle \otimes \varrho^a \oplus \langle -a \rangle \otimes \varrho^a \approx_K \langle a, -a \rangle \otimes \varrho^a \approx_K \langle 1, -1 \rangle \otimes \varrho^a \sim_K 0$, 与 K 的选取矛盾. 因此, 对于某个自然数 n, $2^n \times q \sim_F 0$. 证毕.

剩余环 $W(F)/\mathrm{Nil}(W(F))$ 称作域 F 的既约 Witt 环, 且记作 $W(F)_{\mathrm{red}}$. 由环同态基本定理, 我们有一个从环 $W(F)_{\mathrm{red}}$ 到 $C(\mathcal{X}_F, \mathbb{Z})$ 的如下嵌入:

$$[q] + \mathrm{Nil}(W(F)) \longmapsto \mathrm{sgn}([q]).$$

记 $d = \dim(q)$, 且 $\hat{1}$ 是环 $C(\mathcal{X}_F, \mathbb{Z})$ 中单位元, 即 $\hat{1}$ 是像恒为 1 的常量映射. 于是, 对于每个 $P \in \mathcal{X}_F$, $(\mathrm{sgn}([q]) - d\hat{1})(P) = \mathrm{sgn}_P([q]) - d = \mathrm{sgn}_P(q) - d \in 2\mathbb{Z}$. 从而 $\mathrm{sgn}([q]) - d\hat{1} \in C(\mathcal{X}_F, 2\mathbb{Z})$, 即 $\mathrm{sgn}([q]) \in d\hat{1} + C(\mathcal{X}_F, 2\mathbb{Z}) \subseteq \mathbb{Z} \cdot \hat{1} + C(\mathcal{X}_F, 2\mathbb{Z})$. 因此, 上面的嵌入实际上为 $W(F)_{\mathrm{red}}$ 到子环 $\mathbb{Z} \cdot \hat{1} + C(\mathcal{X}_F, 2\mathbb{Z})$ 的一个嵌入. 换言之, 同态 sgn 的像包含在子环 $\mathbb{Z} \cdot \hat{1} + C(\mathcal{X}_F, 2\mathbb{Z})$ 中.

第六章　特殊的实域与序域

在本章中，将介绍和讨论几种重要的实域与序域，这些域具有特殊的重要性质. 关于这些特殊实域与序域的研究不仅促使实域理论的深化，同时也丰富了一般域论和二次型理论.

§6.1　SAP 域

在这一节中，我们将研究一类特殊实域 —SAP 域，从而得到这类实域的许多特性. 研究的结果表明，这类实域恰好是定义 5.5.8 中所说的满足弱 Hasse 原理 (即 WH) 的域.

在给出 SAP 域的定义之前，我们先考察实域的序空间的两个不相交子集的分离情况. 设 F 是一个实域， A 和 B 是序空间 $\mathcal{X}_F$ 的两个子集. 如果有 $a \in \dot{F}$, 使得 $A \subseteq H(a)$, 但 $B \subseteq H(-a)$, 那么称 A 和 B 可被元素 a 分离，或简称 A 和 B 可分离.

若 $A = \{P_1\}$, 且 $B = \{P_2\}$, 其中 $P_1 \neq P_2$, 则对于 $a \in P_1 \setminus P_2$, A 和 B 可被 a 分离. 若 $A = \{P_1\}$, $B = \{P_2, P_3\}$, 且 $A \cap B = \phi$, 则由刚才的事实知， $\{P_1\}$ 和 $\{P_2\}$ 可被 b 分离，且 $\{P_1\}$ 和 $\{P_3\}$ 可被 c 分离，其中 $b, c \in \dot{F}$. 当 $b \notin P_3$ 或 $c \notin P_2$ 时， A 和 B 可被 b 或 c 分离. 当 $b \in P_3$ 且 $c \in P_2$ 时， A 和 B 可被 bc 分离. 若 $A = \{P_1, P_2\}$, $B = \{P_3, P_4\}$, 且 $A \cap B = \phi$, 则由刚才的事实知， $\{P_1\}$ 和 B 可被 b 分离，且 $\{P_2\}$ 和 B 可被 c 分离，其中 $b, c \in \dot{F}$. 当 $b \in P_2$ 或 $c \in P_1$ 时， A 和 B 可被 b 或 c 分离；当 $b \notin P_2$ 且 $c \notin P_1$ 时， A 和 B 可被 $-bc$ 分离.

然而，下面的例子表明：在一般情况下，不可能把一个正锥和另外三个相异的正锥分离.

例　设 $F = \mathbb{R}((x))((y))$ 是实数域 $\mathbb{R}$ 上双重幂级数域. F 的每个正锥惟一地由元素 x 和 y 的符号惟一确定. 从而 $|\mathcal{X}_F| = 4$, 即 $\mathcal{X}_F = \{P_1, P_2, P_3, P_4\}$. 假若 $\{P_1\}$ 和 $\{P_2, P_3, P_4\}$ 可被 a 分离，其中 $a \in \dot{F}$. 容易证明 $\dot{F} = \bigcup\limits_z z\dot{F}^2$, 其中 z 取遍 $\{\pm 1, \pm x, \pm y, \pm xy\}$ 中八个元素. 从而对于某个 $z_1 \in \{\pm 1, \pm x, \pm y, \pm xy\}$, $a \in z_1\dot{F}^2$. 此时, 显然 $\{P_1\}$ 和 $\{P_2, P_3, P_4\}$ 可被 z_1 分离. 然而, 可逐一地验证： $\{\pm 1, \pm x, \pm y, \pm xy\}$ 中任意一个元素都不可能分离 $\{P_1\}$ 和 $\{P_2, P_3, P_4\}$. 所导致的矛盾表明， $\{P_1\}$ 和 $\{P_2, P_3, P_4\}$ 是不可能分离的.

现在，我们给出 SAP 域的定义如下.

定义 6.1.1　设 F 是一个实域. 如果序空间 $\mathcal{X}_F$ 的任意两个不相交的闭子集都可分离，那么称 F 是一个具有强逼近性质的域. 此时，常简称 F 是一个 SAP 域.

显然，实闭域是 SAP 域. 更一般地，由上面讨论知，每个满足 $|\mathcal{X}_F| < 4$ 的实域是 SAP 域. 然而，上面例子中的实域不是 SAP 域.

通过拓扑学知识，容易建立下面结果.

命题 6.1.1　对于一个实域 F, 下列叙述等价:

(1) F 是一个 SAP 域;

(2) 在序空间 $\mathcal{X}_F$ 中，子基 $\mathcal{H} = \{H(a) \mid a \in \dot{F}\}$ 对于有限交是封闭的，即 $\mathcal{H}$ 是 $\mathcal{X}_F$ 的一个基;

(3) $\mathcal{X}_F$ 的每个既开又闭的子集属于 $\mathcal{H}$.

证明　(1) $\Longrightarrow$ (3): 设 W 是 $\mathcal{X}_F$ 的一个既开又闭的子集，则 W 和 $\mathcal{X}_F \setminus W$ 是 $\mathcal{X}_F$ 的不相交的两个闭子集. 由叙述 (1) 知，有 $a \in \dot{F}$, 使得 $W \subseteq H(a)$, 而 $\mathcal{X}_F \setminus W \subseteq H(-a)$. 此时显然有，$W = H(a) \in \mathcal{H}$.

(3) $\Longrightarrow$ (2): 注意到，$\mathcal{H}$ 中任意有限个成员的交集是 $\mathcal{X}_F$ 的既开又闭的子集. 由叙述 (3) 知，叙述 (2) 成立.

(2) $\Longrightarrow$ (1): 设 A 和 B 是 $\mathcal{X}_F$ 的两个不相交的闭子集，则 $\mathcal{X}_F \setminus A$ 是开子集，且 $B \subseteq \mathcal{X}_F \setminus A$. 由叙述 (2) 知，$\mathcal{H}$ 是序空间 $\mathcal{X}_F$ 的一个基. 从而对于每个 $P \in B$, 有 $H_P \in \mathcal{H}$, 使得 $P \in H_P \subseteq \mathcal{X}_F \setminus A$. 于是，有 B 的一个开复盖: $B \subseteq \bigcup\limits_{P\in B} H_P$. 由定理 1.5.3 知，$\mathcal{X}_F$ 是一个 Hausdorff 紧空间. 从而闭子集 B 是 $\mathcal{X}_F$ 的一个紧子集. 于是，存在有限个 $P_1, \cdots, P_n \in B$, 使得 $B \subseteq \bigcup\limits_{i=1}^{n} H_{P_i}$. 记 $H_{P_i} = H(a_i)$, 其中 $a_i \in \dot{F}$, $i = 1, \cdots, n$. 此时易知，$A \subseteq H(-a_1) \cap \cdots \cap H(-a_n)$, 且 $B \cap H(-a_1) \cap \cdots \cap H(-a_n) = \varnothing$. 再由叙述 (2) 知，$H(-a_1) \cap \cdots \cap H(-a_n) \in \mathcal{H}$, 即有 $a \in \dot{F}$, 使得 $H(-a_1) \cap \cdots \cap H(-a_n) = H(a)$. 从而，$A$ 和 B 可被 a 分离. 证毕.

现在，我们可以给出 SAP 域的如下刻画性质.

定理 6.1.2　设 F 是一个实域，则下列叙述等价:

(1) F 是一个 SAP 域;

(2) $\mathcal{X}_F$ 中任意一个正锥和不包含这一正锥的所有闭子集可分离;

(3) $\mathcal{X}_F$ 的任意两个不相交的有限子集可分离;

(4) $\mathcal{X}_F$ 的任意一个非阿基米德正锥和其他任意三个非阿基米德正锥可分离;

(5) 对于 F 的每个实赋值 v, $|G_v/2G_v| \leqslant 2$, 且当 $|G_v/2G_v| = 2$ 时，$|\mathcal{X}_{F_v}| = 1$;

(6) $\mathcal{X}_F = \mathcal{Y}_F$;

(7) F 满足 WH.

证明　论证途径为: (1) $\Longrightarrow$ (2) $\Longrightarrow$ (4) $\Longrightarrow$ (5) $\Longrightarrow$ (6) $\Longrightarrow$ (7) $\Longrightarrow$ (1) 以及 (1) $\Longrightarrow$ (3) $\Longrightarrow$ (4). 显然，蕴含关系 “(1) $\Longrightarrow$ (2) $\Longrightarrow$ (4)” 和 “(1) $\Longrightarrow$ (3) $\Longrightarrow$ (4)” 成立.

(6) $\Longleftrightarrow$ (7): 由定理 5.5.12 即知.

(4) $\Longrightarrow$ (5): 设叙述 (5) 不成立, 则有如下两种情况:

情况 1 对于 F 的某个实赋值 v, $|G_v/2G_v|\geqslant 4$. 对于 $g\in G_v$, 记 $\bar{g}=g+2G_v\in G_v/2G_v$. 令 $\mathcal{B}=\{\bar{g}_1,\bar{g}_2,\cdots\}$ 是 $G_v/2G_v$ 作为域 $\mathbb{Z}/2\mathbb{Z}$ 上向量空间的一个基, 且设 $\mathcal{P}$ 是 $G_v/2G_v$ 到 $\mathcal{X}_{F_v}$ 的任意一个取定的常量映射.

按如下条件定义 $\mathrm{Hom}(G_v/2G_v,\{1,-1\})$ 中四个特征标 σ_i, $i=1$, 2,3, 4:

	σ_1	σ_2	σ_3	σ_4
$\bar{g}_1$	1	1	-1	-1
$\bar{g}_2$	1	-1	1	-1
其他	1	1	1	1

设 s 是赋值 v 的一个半截口. 由定理 5.6.6 和定理 5.6.7 知, $\mathcal{P}^{\sigma_i}\in\mathcal{X}_F^v$, $i=1$, 2, 3, 4. 此时可断定, $\mathcal{P}^{\sigma_1}$ 和 $\{\mathcal{P}^{\sigma_2},\mathcal{P}^{\sigma_3},\mathcal{P}^{\sigma_4}\}$ 不能分离. 事实上, 如若不然, 则有 $a\in\dot{F}$, 使得 $a\in\mathcal{P}^{\sigma_1}$, 而 $-a\in\mathcal{P}^{\sigma_i}$, $i=2$, 3, 4.

令 $\overline{v(a)}=n_1\bar{g}_1+n_2\bar{g}_2+\sum\limits_{\bar{g}}n_{\bar{g}}\bar{g}$, 这里 $\sum$ 对基 $\mathcal{B}$ 中除 $\bar{g}_1$ 和 $\bar{g}_2$ 外的其他元素 $\bar{g}$ 求和, 则

$$\sigma_i(\overline{v(a)})=\sigma_i(\bar{g}_1)^{n_1}\cdot\sigma_i(\bar{g}_2)^{n_2},\quad i=1,\ 2,\ 3,\ 4.$$

根据引理 5.6.5 知,

$$a\in\mathcal{P}^{\sigma_i}\Longleftrightarrow as(v(a))^{-1}\sigma_i(\bar{g}_1)^{n_1}\sigma_i(\bar{g}_2)^{n_2}+M_v\in P_0,$$

这里 $P_0=\mathcal{P}(\bar{0})\in\mathcal{X}_{F_v}$, $i=1$, 2, 3, 4.

令 $b=as(v(a))^{-1}$. 注意到, $n_1,n_2\in\{0,1\}$. 从而, 我们有如下表中四种可能.

(n_1,n_2)	$a\in\mathcal{P}^{\sigma_1}$	$-a\in\mathcal{P}^{\sigma_2}$	$-a\in\mathcal{P}^{\sigma_3}$	$-a\in\mathcal{P}^{\sigma_4}$
$(0,0)$	$b+M_v\in P_0$	$b+M_v\notin P_0$	$b+M_v\notin P_0$	$b+M_v\notin P_0$
$(1,0)$	$b+M_v\in P_0$	$b+M_v\notin P_0$	$b+M_v\in P_0$	$b+M_v\in P_0$
$(0,1)$	$b+M_v\in P_0$	$b+M_v\in P_0$	$b+M_v\notin P_0$	$b+M_v\in P_0$
$(1,1)$	$b+M_v\in P_0$	$b+M_v\in P_0$	$b+M_v\in P_0$	$b+M_v\notin P_0$

由上面可见, 每种情形 (每一行) 都产生矛盾. 因此, $\mathcal{P}^{\sigma_1}$ 和 $\{\mathcal{P}^{\sigma_2},\mathcal{P}^{\sigma_3},\mathcal{P}^{\sigma_4}\}$ 不能分离, 即叙述 (4) 不真.

情况 2 $|G_v/2G_v|=2$, 且 F_v 至少有两个不同正锥 P_1 和 P_2. 此时, $G_v/2G_v=\{\bar{0},\bar{g}\}$, 其中 $g\in G_v$, 但 $g\notin 2G_v$. 从而 $\mathrm{Hom}(G_v/2G_v,\{1,-1\})$ 中有两个特征标 σ_1 和 σ_2, 使得 $\sigma_1(\bar{g})=1$, 而 $\sigma_2(\bar{g})=-1$. 令 $\mathcal{P}_i$ 是 $G_v/2G_v$ 到 $\mathcal{X}_{F_v}$ 中值为 P_i 的常量函数, $i=1,2$.

设 s 是 v 的一个半截口. 由定理 5.6.6 和定理 5.6.7 知, $\mathcal{P}_j^{\sigma_i}\in\mathcal{X}_F^v$, $i,j=1,2$. 假设 $\mathcal{P}_1^{\sigma_1}$ 和 $\{\mathcal{P}_1^{\sigma_2},\mathcal{P}_2^{\sigma_1},\mathcal{P}_2^{\sigma_2}\}$ 可分离, 则有 $a\in\dot{F}$, 使得 $a\in\mathcal{P}_1^{\sigma_1}$, 但 $-a\in\mathcal{P}_1^{\sigma_2},\mathcal{P}_2^{\sigma_1},\mathcal{P}_2^{\sigma_2}$.

令 $\overline{v(a)} = n\bar{g}$, 其中 $n = 0$ 或 1, 则 $\sigma_i(\overline{v(a)}) = \sigma_i(\bar{g})^n$, $i = 1, 2$.

令 $b = as(v(a))^{-1}$, 根据引理 5.6.5, 有

$$a \in \mathcal{P}_j^{\sigma_i} \iff b\sigma_i(\bar{g})^n + M_v \in P_j, \quad i, j = 1, 2.$$

当 $n = 0$ 时, $a \in \mathcal{P}_1^{\sigma_1}$ 表明 $b + M_v \in P_1$, 而 $-a \in \mathcal{P}_1^{\sigma_2}$ 表明 $b + M_v \notin P_1$, 矛盾. 当 $n = 1$ 时, $-a \in \mathcal{P}_2^{\sigma_1}$ 表明 $b + M_v \notin P_2$, 而 $-a \in \mathcal{P}_2^{\sigma_2}$ 表明 $b + M_v \in P_2$, 矛盾.

因而, $\mathcal{P}_1^{\sigma_1}$ 和 $\{\mathcal{P}_1^{\sigma_2}, \mathcal{P}_2^{\sigma_1}, \mathcal{P}_2^{\sigma_2}\}$ 不能分离, 即叙述 (4) 不真.

根据上面的论证, 蕴含关系 "(4) $\Longrightarrow$ (5)" 成立.

(5) $\Longrightarrow$ (6): 设叙述 (6) 不真, 即 $\mathcal{X}_F \neq \mathcal{Y}_F$, 则由定理 5.5.12 知, 有 $a, b \in \dot{F}$, 使得型 $q = <1, a, b, -ab>$ 在 F 上不是弱迷向的. 由于 q 关于 F 的每个序都是不定的, 从而由定理 5.8.3 知, F 有一个实赋值 v, 使得 $2G_v \neq G_v$, 且 q 在 (F, v) 的 Hensel 化 (K, w) 上不是弱迷向的. 再由定理 5.5.12 知, $\mathcal{X}_K \neq \mathcal{Y}_K$. 由定理 5.7.6 知, 当 $|G_w/2G_w| = 2$ 时, $|\mathcal{X}_{F_w}| \neq 1$. 由于 (K, w) 是 (F, v) 的直接扩张, 从而可认定 $G_w = G_v$ 且 $F_w = F_v$. 此时有 $|G_v/2G_v| \geqslant 2$, 且当 $|G_v/2G_v| = 2$ 时, $|\mathcal{X}_{F_v}| \neq 1$. 这表明: 叙述 (5) 不真. 因此, 蕴含关系 "(5) $\Longrightarrow$ (6)" 获证.

(7) $\Longrightarrow$ (1): 根据命题 6.1.1, 只须证明: 对于 $a, b \in \dot{F}$, 有 $c \in \dot{F}$, 使得 $H(a) \cap H(b) = H(c)$. 此时, 型 $q = <1, a, -b, ab>$ 关于 F 的每个序都是不定的. 由叙述 (7) 知, q 在 F 上是弱迷向的. 根据命题 5.5.9, S_F 中有不全为零的 s_1, s_2, s_3 和 s_4, 使得

$$s_1 + as_2 - bs_3 + abs_4 = 0.$$

令 $c = as_2 + abs_4 = bs_3 - s_1$. 当 $c \neq 0$ 时, 易知 $H(a) \cap H(b) = H(c)$; 当 $c = 0$ 但 $s_3 \neq 0$ 时, $b \in S_F$, 从而 $H(a) \cap H(b) = H(a)$; 当 $c = s_3 = 0$ 时, $s_1 = 0$. 从而 $s_4 \neq 0$, 进而 $b \in -S_F$. 于是 $H(a) \cap H(b) = \varnothing = H(-1)$. 至此定理获证. 证毕.

根据上面定理以及定理 5.5.7 的推论 2 知, 有理数域 $\mathbb{Q}$ 的任意实代数扩张都是 SAP 域. 此外, 由上面定理, 可进一步得到下面的结论.

定理 6.1.3　设 F 是一个实域, 则下列叙述等价:

(1) F 是一个 SAP 域;

(2) 半序空间 $\mathcal{Y}_F$ 中任意两个不相交的闭子集可分离;

(3) $\mathcal{Y}_F$ 中任意一个半锥和不包含该半锥的所有闭子集可分离;

(4) $\mathcal{Y}_F$ 中每个真半锥和其他任意两个非阿基米德正锥可分离.

证明　显然, 蕴含关系 "(2) $\Longrightarrow$ (3) $\Longrightarrow$ (4)" 成立.

(1) $\Longrightarrow$ (2): 由定理 6.1.2 知, $\mathcal{Y}_F = \mathcal{X}_F$. 此时, 由定义 6.1.1 知, 叙述 (2) 成立.

(4) $\Longrightarrow$ (1): 设叙述 (1) 不成立, 则由定理 6.1.2 知, 定理 6.1.2 中叙述 (5) 不成

立. 从而有如下两种可能情况:

情况 1 对于 F 的某个实赋值 v, $|G_v/2G_v|\geqslant 4$. 同样, 记 $\mathcal{B}=\{\bar{g}_1,\bar{g}_2,\cdots\}$ 是 $\mathbb{Z}/2\mathbb{Z}$ 上向量空间 $G_v/2G_v$ 的一组基, 令 $\mathcal{P}$ 是 $G_v/2G_v$ 到 $\mathcal{X}_{F_v}$ 的任意一个常量映射, 且 $\sigma_2,\sigma_3\in \mathrm{Hom}(G_v/2G_v,\{1,-1\})$, 使得 $\sigma_2(\bar{g}_1)=\sigma_3(\bar{g}_2)=1$, $\sigma_2(\bar{g}_2)=\sigma_3(\bar{g}_1)=-1$, 而对于 $\mathcal{B}$ 中除 $\bar{g}_1$ 和 $\bar{g}_2$ 外的其他元素 $\bar{g}$, $\sigma_2(\bar{g})=\sigma_3(\bar{g})=1$. 对于每个 $\eta\in G_v/2G_v$, η 可惟一地表为 $\eta=k_1\bar{g}_1+k_2\bar{g}_2+\sum\limits_{\bar{g}}k_{\bar{g}}\bar{g}$, 其中 $\sum$ 对 $\mathcal{B}$ 中除 $\bar{g}_1$ 和 $\bar{g}_2$ 外的其他元素 $\bar{g}$ 求和, 且 k_1, k_2, $k_{\bar{g}}=0$ 或 1. 据此, 规定 $\sigma(\eta)=1$, 若 $k_1=k_2=0$; 否则, 规定 $\sigma(\eta)=-1$. 这样, 我们得到 $G_v/2G_v$ 到 $\{1,-1\}$ 的一个映射 σ. 显然, $\sigma\notin \mathrm{Hom}(G_v/2G_v,\{1,-1\})$.

设 s 是 v 的一个半截口. 由定理 5.6.6 和定理 5.6.7 知, $\mathcal{P}^\sigma$ 是 F 的一个真半锥, 且 $\mathcal{P}^{\sigma_2}$, $\mathcal{P}^{\sigma_3}\in\mathcal{X}_F^v$. 由于 v 是非浅显赋值, 从而 $\mathcal{P}^{\sigma_2}$ 和 $\mathcal{P}^{\sigma_3}\in\mathcal{X}_F^v$ 是 F 的两个非阿基米德正锥.

假设 $\mathcal{P}^\sigma$ 和 $\{\mathcal{P}^{\sigma_2},\mathcal{P}^{\sigma_3}\}$ 可分离, 则有 $a\in\dot{F}$, 使得 $a\in\mathcal{P}^\sigma$, 但 $-a\in\mathcal{P}^{\sigma_i}$, $i=2$, 3.

令 $\overline{v(a)}=n_1\bar{g}_1+n_2\bar{g}_2+\sum\limits_{\bar{g}}n_{\bar{g}}\bar{g}$, 其中 $\sum$ 对 $\mathcal{B}$ 中除 $\bar{g}_1$ 和 $\bar{g}_2$ 外的其他元素 $\bar{g}$ 求和. 令 $b=as(v(a))^{-1}$, 由引理 5.6.5 有

$$a\in\mathcal{P}^\sigma\Longleftrightarrow b\sigma(\overline{v(a)})+M_v\in P_0,$$

其中 $P_0=\mathcal{P}(\bar{0})\in\mathcal{X}_{F_v}$.

此时, 我们有如下导致矛盾的表格.

(n_1,n_2)	$a\in\mathcal{P}^\sigma$	$-a\in\mathcal{P}^{\sigma_2}$	$-a\in\mathcal{P}^{\sigma_3}$
$(0,0)$	$b+M_v\in P_0$	$b+M_v\notin P_0$	$b+M_v\notin P_0$
$(1,0)$	$b+M_v\notin P_0$	$b+M_v\notin P_0$	$b+M_v\in P_0$
$(0,1)$	$b+M_v\notin P_0$	$b+M_v\in P_0$	$b+M_v\notin P_0$
$(1,1)$	$b+M_v\notin P_0$	$b+M_v\in P_0$	$b+M_v\in P_0$

因而, $\mathcal{P}^\sigma$ 和 $\{\mathcal{P}^{\sigma_2},\mathcal{P}^{\sigma_3}\}$ 不能分离, 即叙述 (4) 不真.

情况 2 $|G_v/2G_v|=2$, 且 F_v 至少有两个相异的正锥 P_1 和 P_2. 此时, $G_v/2G_v=\{\bar{0},\bar{g}\}$, 其中 $g\in G_v$, 但 $g\notin 2G_v$. 设 $\sigma\in\mathrm{Hom}(G_v/2G_v,\{1,-1\})$, 使得 $\sigma(\bar{0})=\sigma(\bar{g})=1$, $\mathcal{P}_i$ 是 $G_v/2G_v$ 到 $\mathcal{X}_{F_v}$ 的值为 P_i 的常量映射, $i=1,2$. 同时, 规定 $\mathcal{P}_0$ 是 $G_v/2G_v$ 到 $\mathcal{X}_{F_v}$ 的这样一个映射, 使得 $\mathcal{P}_0(\bar{0})=P_1$, 但 $\mathcal{P}_0(\bar{g})=P_2$.

由定理 5.6.6 和定理 5.6.7 知, $\mathcal{P}_0^\sigma$ 是 F 的一个真半锥, 而 $\mathcal{P}_1^\sigma$ 和 $\mathcal{P}_2^\sigma$ 是 F 的两个非阿基米德正锥. 假若 $\mathcal{P}_0^\sigma$ 和 $\{\mathcal{P}_1^\sigma,\mathcal{P}_2^\sigma\}$ 可分离, 则有 $a\in\dot{F}$, 使得 $a\in\mathcal{P}_0^\sigma$, 但 $-a\in\mathcal{P}_i^\sigma$, $i=1,2$.

令 $b=as(v(a))^{-1}$. 注意到 $\sigma(\overline{v(a)})=1$, 从而由引理 5.6.5 有

$$a \in \mathcal{P}_i^{\sigma} \Longrightarrow b + M_v \in \mathcal{P}_i(\overline{v(a)}), \quad i = 0, 1, 2.$$

当 $\overline{v(a)} = \bar{0}$ 时， $a \in \mathcal{P}_0^{\sigma}$ 表明 $b + M_v \in \mathcal{P}_0(\bar{0}) = P_1$, 而 $-a \in \mathcal{P}_1^{\sigma}$ 表明 $b + M_v \notin \mathcal{P}_1(\bar{0}) = P_1$, 矛盾. 当 $\overline{v(a)} = \bar{g}$ 时， $a \in \mathcal{P}_0^{\sigma}$ 表明 $b + M_v \in \mathcal{P}_0(\bar{g}) = P_2$, 而 $-a \in \mathcal{P}_2^{\sigma}$ 表明 $b + M_v \notin \mathcal{P}_2(\bar{g}) = P_2$, 矛盾.

因而， $\mathcal{P}_0^{\sigma}$ 和 $\{\mathcal{P}_1^{\sigma}, \mathcal{P}_2^{\sigma}\}$ 不能分离，即叙述 (4) 不真.

根据上面的论证，蕴含关系 "(4) $\Longrightarrow$ (1)" 成立. 证毕.

推论　设实域 F 的每个实赋值的值群都是 2- 可除的，则 F 的每个实代数扩张都是 SAP 域. 特别地，当 F 仅有阿基米德序或者仅有惟一序时，结论成立.

证明　设 K 是 F 的任意实代数扩张，且 $P \in \mathcal{Y}_K$. 对于任意 $a, b \in P$, 令 $L = F(a, b)$, 则 L 是 F 的有限扩张. 设 w 是 L 的任意实赋值，则 $v = w|_K$ 是 F 的一个实赋值. 由所设知， G_v 是 2- 可除的. 注意到 $|G_w/G_v|$ 是一个自然数. 从而易知， G_w 也是 2- 可除的，即 $|G_w/2G_w| = 1$. 因而，域 L 满足定理 5.6.2 中叙述 (5), 从而 $\mathcal{Y}_L = \mathcal{X}_L$. 此时 $a, b \in P \cap L$, 且 $P \cap L \in \mathcal{Y}_L = \mathcal{X}_L$. 由此有 $ab \in P$. 这表明 $P \in \mathcal{X}_K$. 因而 $\mathcal{Y}_K = \mathcal{X}_K$, 即 K 是一个 SAP 域.

当 F 仅有阿基米德序时，由定理 3.2.2 和命题 3.2.3 知，F 仅有浅显的实赋值，相应的值群 $\{0\}$ 显然是 2- 可除的. 当 F 仅有惟一序 P 时，由定理 1.1.3 知，$P = S_F$. 设 v 是 F 的任意实赋值. 对于每个非零 $a \in P$, $a = b_1^2 + \cdots + b_n^2$, 其中 $b_i \in F, i = 1, \cdots, n$. 由命题 3.1.2 知， $v(a) = \min\{v(b_i^2) \mid i = 1, \cdots, n\} = 2\min\{v(b_i) \mid i = 1, \cdots, n\} \in 2G_v$. 从而 $G_v = 2G_v$. 因此，推论中后一叙述成立. 证毕.

在 §5.9 中，借助于全符号差，我们可规定实域 F 的 Witt 环 $W(F)$ 到连续映射环 $C(\mathcal{X}_F, \mathbb{Z})$ 的一个同态 sgn: $[q] \longmapsto \mathrm{sgn}([q])$. 在研究同态核 $ker(\mathrm{sgn})$ 后，我们还指出这样一个事实：同态像 $\mathrm{sgn}(W(F)) \subseteq \mathbb{Z} \cdot \hat{1} + C(\mathcal{X}_F, 2\mathbb{Z})$, 其中 $\hat{1}$ 是值恒为 1 的常量映射.

下面定理通过 Witt 环给出了 SAP 域的另一个重要刻画：

定理 6.1.4　设 F 是一个实域， sgn 是 $W(F)$ 到 $C(\mathcal{X}_F, \mathbb{Z})$ 的全符号差同态，则 F 是 SAP 域，当且仅当 $\mathrm{sgn}(W(F)) = \mathbb{Z} \cdot \hat{1} + C(\mathcal{X}_F, 2\mathbb{Z})$.

证明　必要性：设 F 是 SAP 域. 由于 $\hat{1} = \mathrm{sgn}([\langle 1 \rangle]) \in \mathrm{sgn}(W(F))$, 从而只需证明： $C(\mathcal{X}_F, 2\mathbb{Z}) \subseteq \mathrm{sgn}(W(F))$. 设 $f \in C(\mathcal{X}_F, 2\mathbb{Z})$, 则对于每个 $n \in \mathbb{Z}$, $f^{-1}(2n)$ 是 $\mathcal{X}_F$ 的既开又闭的子集. 从而， $\mathcal{X}_F$ 有这样一个开复盖： $\mathcal{X}_F \subseteq \bigcup\limits_{n \in \mathbb{Z}} f^{-1}(2n)$. 由于 $\mathcal{X}_F$ 是紧空间，从而有有限个 $n_1, \cdots, n_r \in \mathbb{Z}$, 使得 $\mathcal{X}_F = \bigcup\limits_{i=1}^{r} f^{-1}(2n_i)$. 由命题 6.1.1 知，有 $a_i \in \dot{F}$, 使得 $f^{-1}(2n_i) = H(a_i)$, $i = 1, \cdots, r$. 令 $q = \bigoplus\limits_{i=1}^{r} n_i \times \langle 1, a_i \rangle$, 则 $[q] \in W(F)$. 对于任意 $P \in \mathcal{X}_F$, 必有某个 $k \in \{1, \cdots, r\}$, 使得 $P \in f^{-1}(2n_k)$, 即 $f(P) = 2n_k$. 此时显然 $a_k \in P$, 但 $a_i \notin P$, 只要 $i \neq k$. 从而 $\mathrm{sgn}([q])(P) = \mathrm{sgn}_P(q) =$

$\sum_{i=1}^{r} \mathrm{sgn}_P(n_i \times \langle 1, a_i\rangle) = 2n_k$. 因而 $f = \mathrm{sgn}([q]) \in \mathrm{sgn}(W(F))$. 必要性获证.

充分性：设 $\mathrm{sgn}(W(F)) = \mathbb{Z}\cdot\hat{1} + C(\mathcal{X}_F, 2\mathbb{Z})$. 对于 $\mathcal{X}_F$ 的任意一个既开又闭子集 A, 规定 $\mathcal{X}_F$ 到 $2\mathbb{Z}$ 的这样一个映射 f, 使得 $f(P) = 0$, 若 $P \in A$; 而 $f(P) = 2$, 若 $P \in \mathcal{X}_F \setminus A$. 显然, $f \in C(\mathcal{X}_F, 2\mathbb{Z}) \subseteq \mathrm{sgn}(W(F))$. 从而有 F 上正则型 q, 使得 $f = \mathrm{sgn}([q])$. 从而对于每个 $P \in \mathcal{X}_F$, $f(P) = \mathrm{sgn}_P(q)$. 显然, $\dim(q)$ 是一个偶数. 从而可设 $q = \langle a_1, \cdots, a_{2m}\rangle$, 其中 $a_1, \cdots, a_{2m} \in \dot{F}$.

令 $a = (-1)^m a_1 a_2 \cdots a_{2m}$, 则 $P \in A$, 当且仅当 $\mathrm{sgn}_P(q) = f(P) = 0$, 即 $a_1, \cdots, a_{2m}$ 中恰有 m 个元素关于 P 的符号为负, 当且仅当 $a \in P$. 因而, $A = H(a)$. 由命题 6.1.1 知, F 是一个 SAP 域. 证毕.

§6.2 欧 氏 域

在这一节中, 将介绍一种特殊实域 —— 欧氏域. 欧氏域可以看作关于二次扩张的实闭域.

定义 6.2.1 一个实域 F 称作欧几里得域，若 $F = F^2 \cup -F^2$. 此时, 简称 F 为欧氏域.

显然, 对于一个欧氏域 F, F 有惟一正锥 F^2. 实闭域显然为欧氏域. 作为不是实闭的欧氏域, 我们给出下面例子.

例 设 E 是全体可通过规尺构作的实数组成的集合. 由规定, $0, 1 \in E$. 对于 $\alpha, \beta \in E$, 显然 $\alpha \pm \beta \in E$. 此外, 由比例线段的作图知, $\alpha\beta = \dfrac{\alpha\cdot\beta}{1} \in E$, 且当 $\alpha \neq 0$ 时, $\alpha^{-1} = \dfrac{1\cdot 1}{\alpha} \in E$. 因而 E 是实数域 $\mathbb{R}$ 的一个子域.

设 $\alpha \in E$, 且 $\alpha > 0$. 由线段比例中项的作图可知, $\sqrt{\alpha} = \sqrt{\alpha\cdot 1} \in E$. 因而有 $E = E^2 \cup -E^2$, 即 E 是一个欧氏域. 然而, 作为一个熟知的不可作图问题, $\sqrt[3]{2} \notin E$. 因此, E 不是实闭的.

设 F 是任意域, Ω 是 F 的代数闭包. 规定 Ω 的如下非空子集:

$$\sqrt{F} = \{\alpha \in \Omega \mid \alpha^2 \in F\}.$$

据此, 我们可以归纳地构造 F 和 Ω 的中间域 F_n, 其中 n 为非负整数, 使得 $F_0 = F$, $F_{n+1} = F_n(\sqrt{F_n})$. 显然, $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \subseteq \cdots$. 令 $F\langle 2\rangle = \bigcup_{n=0}^{\infty} F_n$, 则 $F\langle 2\rangle$ 为 F 和 Ω 的中间域. 这个中间域 $F\langle 2\rangle$ 具有如下重要性质:

(1)$F\langle 2\rangle$ 是二次闭域, 即 $F\langle 2\rangle$ 没有二次扩张 (也即 $F\langle 2\rangle^2 = F\langle 2\rangle$).

事实上, 对于每个 $\alpha \in F\langle 2\rangle$, 由 $F\langle 2\rangle$ 的构造知, 有某个非负整数 n, 使得 $\alpha \in F_n$. 由于 Ω 是代数闭域, 从而有 $\beta \in \Omega$, 使得 $\beta^2 = \alpha$. 此时, $\beta \in \sqrt{F_n} \subseteq F_{n+1} \subseteq F\langle 2\rangle$.

从而 $\alpha=\beta^2\in F\langle 2\rangle^2$.

(2)F 和 $F\langle 2\rangle$ 的每个不等于 $F\langle 2\rangle$ 的中间域不是二次闭域.

事实上，若 K 是 F 和 $F\langle 2\rangle$ 的一个中间域，且 $K\neq F\langle 2\rangle$, 则存在某个非负整数 m, 使得 $F_m\not\subseteq K$. 由非负整数的良序性，这个 m 可选取尽可能小. 由于 $F_0=F\subseteq K$, 从而 $m>0$. 由 m 的选取知，$F_{m-1}\subseteq K$, 但 $F_{m-1}(\sqrt{F_{m-1}})\not\subseteq K$. 于是，至少有一个 $\alpha\in\sqrt{F_{m-1}}$, 使得 $\alpha\notin K$. 此时 $\alpha^2\in F_{m-1}\subseteq K$. 因此，$K(\alpha)$ 是 K 的一个二次扩张，即 K 不是二次闭域.

定义 6.2.2　域 F 的一个代数扩张 K 称作域 F 的一个二次闭包，如果 K 满足这样两个性质：(1)K 是二次闭域；(2)F 和 K 的每个不等于 K 的中间域不是二次闭域.

上面的讨论表明了任意域的二次闭包的存在性. 作为二次闭包的惟一性，可给出如下命题.

命题 6.2.1　域 F 的任意两个二次闭包都是 F- 同构的.

证明　设 K 是域 F 的任意一个二次闭包，且 Ω_1 是 K 的代数闭包，则 Ω_1 显然也是 F 的代数闭包. 由代数闭包的惟一性知，存在 Ω 到 Ω_1 的一个 F- 同构 π, 这里 Ω 是上面所给定的 F 的代数闭包. 由上面讨论知，$F\langle 2\rangle$ 是 Ω 中二次闭域. 从而，$\pi(F\langle 2\rangle)$ 是 Ω_1 中的二次闭域. 注意这样一个事实：二次闭域的交集仍是二次闭域. 从而 $\pi(F\langle 2\rangle)\cap K$ 是一个二次闭域，且 $F\subseteq\pi(F\langle 2\rangle)\cap K\subseteq K$. 由定义 6.2.2 中性质 (2) 知，$\pi(F\langle 2\rangle)\cap K=K$, 即有 $K\subseteq\pi(F\langle 2\rangle)$. 同样有 $F\langle 2\rangle\subseteq\pi^{-1}(K)$, 即有 $\pi(F\langle 2\rangle)\subseteq K$. 因此，$\pi(F\langle 2\rangle)=K$. 这表明：$\pi$ 在 $F\langle 2\rangle$ 上的限制是 $F\langle 2\rangle$ 到 K 的一个 F- 同构. 证毕.

根据命题 6.2.1, 在措辞 "域 F 的一个二次闭包" 中，不定冠词 "一个" 可省略. 对于域的二次闭包，我们有如下基本结果.

命题 6.2.2　设 $F\langle 2\rangle$ 是域 F 的二次闭包，则

(1)$F\langle 2\rangle$ 是 F 的正规扩张，且当 F 的特征 $\neq 2$ 时，$F\langle 2\rangle$ 是 F 的 Galois 扩张；

(2)F 是二次闭的，当且仅当 $F=F\langle 2\rangle$;

(3) 若 K 是 F 的一个二次闭扩张，且 K 和 $F\langle 2\rangle$ 包含在同一扩域中，则 $F\langle 2\rangle\subseteq K$;

(4) 若 K 是 F 和 $F\langle 2\rangle$ 的中间域，且 K 是 F 的有限扩张，则扩张次数 $[K:F]$ 是 2 的方幂.

证明　(1) 设 Ω 是 $F\langle 2\rangle$ 的代数闭包，且 π 是 Ω 的任意一个 F- 自同构. 显然，Ω 也是 F 的代数闭包. 根据命题 6.2.1 的证明，类似地可证：$\pi(F\langle 2\rangle)=F\langle 2\rangle$. 这表明 $F\langle 2\rangle$ 为 F 的正规扩张.

当 F 的特征 $\neq 2$ 时，对于每个非负整数 n, $\sqrt{F_n}$ 中每个元素都是域 F_n 上可分代数元. 从而 $F_{n+1} = F_n(\sqrt{F_n})$ 是 F_n 的可分扩张. 由可分扩张的传递性知，对于每个 n, F_n 是 F 的可分扩张. 因而， $F\langle 2\rangle$ 为 F 的可分扩张. 叙述 (1) 获证.

(2) 显然叙述 (2) 成立.

(3) 此时， $F \subseteq K \cap F\langle 2\rangle \subseteq F\langle 2\rangle$, 且 $K \cap F\langle 2\rangle$ 也是二次闭域. 根据定义 6.2.2 中性质 (2) 知， $K \cap F\langle 2\rangle = F\langle 2\rangle$. 因此， $F\langle 2\rangle \subseteq K$.

(4) 先证这样一个事实：对于 $\alpha \in F\langle 2\rangle$, $[F(\alpha):F]$ 是 2 的方幂. 事实上，由于 $\alpha \in F\langle 2\rangle$, 从而有某个非负整数 k, 使得 $\alpha \in F_k$. 此时， $[F_k(\alpha):F_k] = 1 = 2^0$ 是 2 的方幂. 选取最小非负整数 m, 使得 $[F_m(\alpha):F_m]$ 是 2 的方幂. 假设 $m > 0$, 则 $F_m = F_{m-1}(\sqrt{F_{m-1}})$. 令 α 在 F_m 上的极小多项式为

$$f(x) = x^{2^r} + \alpha_1 x^{2^r - 1} + \cdots + \alpha_{2^r},$$

其中 $\alpha_1, \cdots, \alpha_{2^r} \in F_m$. 从而有有限个元素 $\beta_1, \cdots, \beta_n \in \sqrt{F_m}$, 使得 $\alpha_i \in F_{m-1}(\beta_1, \cdots, \beta_n)$, $i = 1, \cdots, 2^r$.

显然， $[F_{m-1}(\beta_1, \cdots, \beta_{j-1}, \beta_j) : F_{m-1}(\beta_1, \cdots, \beta_{j-1})] = 2$ 或 1, $j = 1, \cdots, n$. 从而 $[F_{m-1}(\beta_1, \cdots, \beta_n) : F_{m-1}] = 2^s$, 其中 $s \geqslant 0$. 由于 $f(x)$ 在 $F_{m-1}(\beta_1, \cdots, \beta_n)$ 上是不可约的，从而 $[F_{m-1}(\beta_1, \cdots, \beta_n, \alpha) : F_{m-1}(\beta_1, \cdots, \beta_n)] = 2^r$. 于是有

$$[F_{m-1}(\beta_1, \cdots, \beta_n, \alpha) : F_{m-1}] = 2^{r+s}.$$

注意到， $[F_{m-1}(\alpha) : F_{m-1}]$ 是 $[F_{m-1}(\beta_1, \cdots, \beta_n, \alpha) : F_{m-1}]$ 的一个因数. 从而 $[F_{m-1}(\alpha) : F_{m-1}]$ 是 2 的方幂，矛盾于 m 的选取. 因而， $m = 0$, 即 $[F(\alpha):F]$ 是 2 的方幂.

现设 $K = F(\alpha_1, \cdots, \alpha_s)$, 其中 $\alpha_1, \cdots, \alpha_s \in F\langle 2\rangle$. 注意到， $F\langle 2\rangle$ 也是域 $F(\alpha_1, \cdots, \alpha_{s-1})$ 的二次闭包. 由上面的已证事实知， $[K : F(\alpha_1, \cdots, \alpha_{s-1})]$ 为 2 的方幂. 借助于归纳假定，可设 $[F(\alpha_1, \cdots, \alpha_{s-1}) : F]$ 为 2 的方幂. 从而， $[K:F]$ 为 2 的方幂. 证毕.

现在来讨论欧氏域. 下面定理给出了欧氏域的一系列刻画性质.

定理 6.2.3 对于一个实域 F, 下列叙述是等价的：

(1) F 为欧氏域;

(2) $F^2 + F^2 \subseteq F^2$, 且 F 有惟一序;

(3) $F(\sqrt{-1})$ 是二次闭域;

(4) F 有一个二次闭的有限扩张;

(5) F 的所有二次扩张都不是实域;

(6) Witt 环 $W(F)$ 同构于整数环 $\mathbb{Z}$;

(7) Witt 环 $W(F)$ 是一个整环.

证明 证明的途径为：(1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) $\Longrightarrow$ (4) $\Longrightarrow$ (3) $\Longrightarrow$ (5) $\Longrightarrow$ (1) 和 (1) $\Longrightarrow$ (6) $\Longrightarrow$ (7) $\Longrightarrow$ (1). 显然，如下蕴含关系成立：(1) $\Longrightarrow$ (2), (3) $\Longrightarrow$ (4), (3) $\Longrightarrow$ (5) 和 (6) $\Longrightarrow$ (7).

(2) $\Longrightarrow$ (3): 由于 F 有惟一序，从而由定理 1.1.3 的推论知，S_F 是 F 的惟一正锥. 又由于 $F^2+F^2\subseteq F^2$, 从而 $S_F=F^2$. 于是，$F=F^2\cup -F^2$. 再由引理 2.1.2 知，$F(\sqrt{-1})$ 是二次闭域.

(4) $\Longrightarrow$ (3): 设 K 是 F 的一个二次闭的有限扩张，Ω 是 K 的代数闭包，则 Ω 也是 F 的代数闭包. 令 $F\langle 2\rangle$ 是 F 在 Ω 中的二次闭包. 由命题 6.2.2 知 $F\langle 2\rangle\subseteq K$, 且 $F\langle 2\rangle$ 是 F 的 Galois 扩张. 再由命题 6.2.2(4) 可知，$[F\langle 2\rangle : F(\sqrt{-1})]=2^r$, 其中 r 为非负整数. 假若 $r>0$, 则 Galois 群 $\mathrm{Aut}(F\langle 2\rangle/F(\sqrt{-1}))$ 有一个阶为 2 的子群 H. 令 L 是 H 的稳定子域，则由 Galois 基本定理知，$F(\sqrt{-1})\subseteq L\subseteq F\langle 2\rangle$, 且 $[F\langle 2\rangle : L]=2$. 由于 F 的特征为零，从而有 $\alpha\in F\langle 2\rangle$, 使得 $F\langle 2\rangle=L(\alpha)$, 且 $\alpha^2\in L$. 由于 $F\langle 2\rangle$ 是二次闭的，从而 $\sqrt{\alpha}\in F\langle 2\rangle=L(\alpha)$, 即 $\sqrt{\alpha}=a+b\alpha$, 其中 $a,b\in L$. 由此有 $\alpha=(a^2+b^2\alpha^2)+(2ab)\alpha$. 注意到，$1,\alpha$ 在 L 上线性无关. 从而 $a^2+b^2\alpha^2=0$, 且 $2ab=1$. 于是 $b\neq 0$, 且 $\alpha=\pm ab^{-1}\sqrt{-1}\in L$, 矛盾. 因而，$r=0$, 即 $F(\sqrt{-1})=F\langle 2\rangle$. 自然，$F(\sqrt{-1})$ 是二次闭域.

(5) $\Longrightarrow$ (1): 由于 F 是实域，从而 F 有一个正锥 P. 令 R 是序域 (F,P) 的实闭包. 对于每个 $a\in P$, $\sqrt{a}\in R$. 从而 $F(\sqrt{a})$ 是 F 的实扩张. 显然，$[F(\sqrt{a}):F]\leqslant 2$. 由叙述 (5) 知，$[F(\sqrt{a}):F]\neq 2$; 否则 $F(\sqrt{a})$ 不是实域. 因而 $[F(\sqrt{a}):F]=1$, 即 $\sqrt{a}\in F$. 由此有，$a=(\sqrt{a})^2\in F^2$. 此时有 $P=F^2$, 即有 $F=F^2\cup -F^2$. 因此，F 为欧氏域.

(1) $\Longrightarrow$ (6): 由于 F 是欧氏域，从而 F^2 是 F 的惟一序. 考虑 Witt 环 $W(F)$ 到 $\mathbb{Z}$ 的符号差满同态

$$\mathrm{sgn}_{F^2}:\quad [q]\longmapsto \mathrm{sgn}_{F^2}(q),\quad [q]\in W(F).$$

设 $[q]\in\ker(\mathrm{sgn}_{F^2})$, 其中 $q=\langle a_1,\cdots,a_n\rangle$ 是 F 上一个正则型，则 $\mathrm{sgn}_{F^2}(\langle a_1,\cdots,a_n\rangle)=0$. 此时 $n=2m$ 为偶数，且 $a_1,\cdots,a_{2m}$ 中恰有 m 个元素属于 F^2. 不妨设 $a_1,\cdots,a_m\in F^2$, 而 $a_{m+1},\cdots,a_{2m}\in -F^2$. 于是 $q\approx_F <1,\cdots,1,-1,\cdots,-1>$, 即 q 是双曲型. 从而 $[q]=[0]$. 因此，sgn_{F^2} 是一个环同构.

(7) $\Longrightarrow$ (1): 对于每个 $a\in\dot{F}$, 在环 $W(F)$ 中，$([\langle a\rangle]-[\langle 1\rangle])\otimes([\langle a\rangle]-[\langle -1\rangle])=[\langle a^2\rangle]-[\langle -a\rangle]-[\langle a\rangle]+[\langle -1\rangle]=[\langle a^2,-1\rangle]=[\langle 1,-1\rangle]=[0]$. 由所设，$W(F)$ 是整环. 从而 $[\langle a\rangle]=[\langle 1\rangle]$ 或 $[\langle a\rangle]=[\langle -1\rangle]$. 此时必有 $\langle a\rangle\approx_F\langle 1\rangle$ 或 $\langle a\rangle\approx_F\langle -1\rangle$. 由此有 $a\in\dot{F}^2$ 或 $a\in-\dot{F}^2$. 因此，F 为欧氏域. 至此定理获证. 证毕.

推论 设 K 是域 F 的一个有限扩张，且 K 是一个欧氏域，则 F 也是欧氏域.

证明 由定理 6.2.3 知，$K(\sqrt{-1})$ 是二次闭域. 这样，F 有一个二次闭的有限扩张 $K(\sqrt{-1})$. 再由定理 6.2.3 知，F 是一个欧氏域. 证毕.

很清楚，并非每个实域都是欧氏域，但每个实域都有一个欧氏扩张，比如它的任意实闭包. 然而，有研究意义的欧氏扩张是如下所说的 "最小" 欧氏扩张.

定义 6.2.3 域 F 的一个代数扩张 E 称作 F 的一个欧氏包，如果 E 为欧氏域，且 F 和 E 的每个不等于 E 的中间域不再为欧氏域.

显然，一个域 F 为欧氏域，当 F 是它自身的惟一欧氏包. 立足于定义 6.2.3, 首要任务自然是证明下面结论.

命题 6.2.4 设 F 是一个实域，则有

(1) F 的欧氏包总是存在的;

(2) 若 E_1 和 E_2 都是 F 的欧氏包，则 E_1 和 E_2 是 F- 同构，当且仅当 $E_1^2 \cap F = E_2^2 \cap F$.

证明 (1) 由于 F 是一个实域，从而 F 有一个实闭包 R. 由定理 2.1.3 知，$R(\sqrt{-1})$ 是 F 的代数闭包. 设 $F\langle 2\rangle$ 是 F 在 $R(\sqrt{-1})$ 中的二次闭包，且令 $E = R\cap F\langle 2\rangle$, 则 E 显然是 F 的一个实代数扩张. 对于 $e \in E$, 由 $F\langle 2\rangle$ 的二次闭性知，有 $\alpha, \beta \in F\langle 2\rangle$, 使得 $e = \alpha^2$, 而 $-e = \beta^2$. 当 $e \in R^2$ 时，有 $u \in R$, 使得 $e = u^2$. 由此知，$\alpha = \pm u \in R \cap F\langle 2\rangle = E$, 从而 $e \in E^2$. 当 $e \in -R^2$ 时，类似可得 $e \in -E^2$. 因此，E 是一个欧氏域.

设 L 是 F 和 E 的任意一个中间域，且 L 是欧氏域. 由定理 6.2.3 知，$L(\sqrt{-1})$ 是一个二次闭域. 再由命题 6.2.2(3) 知，$F\langle 2\rangle \subseteq L(\sqrt{-1})$. 由此有，$E = F\langle 2\rangle \cap R \subseteq L(\sqrt{-1}) \cap R = L$, 即有 $E = L$. 由定义 6.2.3 知，E 为 F 的一个欧氏包.

(2) 必要性显然，下证充分性. 设 R_1 和 R_2 分别为序域 (E_1, E_1^2) 和 (E_2, E_2^2) 的实闭包. 由所设知，R_1 和 R_2 都是序域 (F, P) 的实闭包，这里 $P = E_1^2 \cap F = E_2^2 \cap F$. 由实闭包的惟一性，存在 R_1 到 R_2 的一个 F- 同构 π. 由于 E_1 是 R_1 中欧氏域，从而 $\pi(E_1)$ 也是 R_2 中欧氏域. 注意到这样一个事实: 同一实域中欧氏子域的交集还是欧氏子域. 从而 $\pi(E_1) \cap E_2$ 是欧氏域，且 $F \subseteq \pi(E_1) \cap E_2 \subseteq E_2$. 由定义 6.2.3 知，$\pi(E_1) \cap E_2 = E_2$, 即 $E_2 \subseteq \pi(E_1)$. 同样有，$E_1 \subseteq \pi^{-1}(E_2)$. 从而，$\pi(E_1) \subseteq E_2$. 因此，$\pi$ 在 E_1 上的限制为 E_1 到 E_2 的 F- 同构. 证毕.

由上面定理的证明可见，实域 F 在它的每个实闭包中恰有一个欧氏包. 此外，若 R_1 和 R_2 是 F 的两个实闭包，E_1 和 E_2 分别是 F 在 R_1 和 R_2 中的欧氏包，且 E_1 和 E_2 是 F- 同构的，则 $R_1^2 \cap F = (R_1^2 \cap E_1) \cap F = E_1^2 \cap F = E_2^2 \cap F = R_2^2 \cap F$. 从而 R_1 和 R_2 都是序域 $(F, R_1^2 \cap F)$ 的实闭包. 由实闭包的惟一性知，R_1 和 R_2 是 F- 同构的. 因此，对于一个实域 F, 所有欧氏包的 F- 同构类与所有实闭包的 F- 同构类之间存在一一对应.

推论 1 设 F 是一个实域，则 F 的欧氏包在 F- 同构的意义下是惟一的，当

且仅当 F 只有惟一序.

推论 2 设 P 是 F 的一个正锥, 则 F 的所有使得 $P \subseteq E^2$ 的欧氏包 E 是 F-同构的.

下面定理给出了欧氏包的刻画性质.

定理 6.2.5 设 E 是实域 F 的一个代数扩张, 且 $F\langle 2\rangle$ 是 F 在 E 的代数闭包 Ω 中的二次闭包, 则下列叙述是等价的:

(1) E 是 F 的一个欧氏包;

(2) E 为欧氏域, 且 $E \subseteq F\langle 2\rangle$;

(3) $F\langle 2\rangle$ 是 E 的二次扩张;

(4) $F\langle 2\rangle$ 是 E 的一个次数大于 1 的有限扩张.

证明 (1) $\Longrightarrow$ (2): 由定义知, E 为欧氏域. 设 R 是序域 (E, E^2) 在 Ω 中的实闭包. 由定理 6.2.4(1) 的证明知, $R \cap F\langle 2\rangle$ 是 F 在 R 中的欧氏包. 从而, 必有 $E = R \cap F\langle 2\rangle \subseteq F\langle 2\rangle$.

(2) $\Longrightarrow$ (3): 由定理 6.2.3 知, $E(\sqrt{-1})$ 是二次闭域. 注意到, $F \subseteq E(\sqrt{-1}) \subseteq F\langle 2\rangle$. 从而由定义 6.2.2 知, $F\langle 2\rangle = E(\sqrt{-1})$. 由于 $\sqrt{-1} \notin E$, 从而 $F\langle 2\rangle$ 是 E 的二次扩张.

(3) $\Longrightarrow$ (4): 显然.

(4) $\Longrightarrow$ (1): 根据定理 6.2.3 中蕴含关系 "(4) $\Longrightarrow$ (3)" 的证明, 可得 $E(\sqrt{-1}) = E\langle 2\rangle$, 这里 $E\langle 2\rangle$ 是 E 在 Ω 中的二次闭包. 从而, $E(\sqrt{-1})$ 是二次闭域. 注意到, $F \subseteq E(\sqrt{-1}) \subseteq F\langle 2\rangle$. 由定义 6.2.2 中性质 (2) 知, $E(\sqrt{-1}) = F\langle 2\rangle$. 由于 $[F\langle 2\rangle : E] > 1$, 从而 $\sqrt{-1} \notin E$, 即 $-1 \notin E^2$. 对于任意 $a, b \in E$, $a + b\sqrt{-1} \in E(\sqrt{-1})$. 由于 $E(\sqrt{-1})$ 是二次闭域, 从而有 $c, d \in E$, 使得 $a + b\sqrt{-1} = (c + d\sqrt{-1})^2$. 由此有 $a^2 + b^2 = (a + b\sqrt{-1})(a - b\sqrt{-1}) = (c + d\sqrt{-1})^2(c - d\sqrt{-1})^2 = (c^2 + d^2)^2 \in E^2$. 于是 $E^2 + E^2 \subseteq E^2$, 即有 $S_E = E^2$. 此时有 $-1 \notin S_E$, 即 E 是一个实域. 由定理 6.2.3 中叙述 (1) 和 (4) 的等价性知, E 是一个欧氏域.

现设 L 是 F 和 E 的中间域, 且 L 是欧氏域. 由定理 6.2.3 知, $L(\sqrt{-1})$ 是二次闭域. 由命题 6.2.2 知, $F\langle 2\rangle \subseteq L(\sqrt{-1})$. 由此有 $E = F\langle 2\rangle \cap E \subseteq L(\sqrt{-1}) \cap E = L$, 即有 $E = L$. 因此, E 是 F 的一个欧氏包. 证毕.

§6.3 遗传欧氏域

在上节, 我们研究了欧氏域. 在本节中, 我们引进和讨论一类满足更强条件的欧氏域 — 遗传欧氏域. 遗传欧氏域与 §6.1 中所讨论的 SAP 域具有密切的联系.

定义 6.3.1 一个域 F 称作遗传欧氏域, 如果 F 及其所有的实代数扩张都是欧氏域.

由定义知，实闭域可作为遗传欧氏域的浅显例子. 对于非浅显的例子，我们将在条件可能的情况下给出.

下面定理给出了遗传欧氏域的一系列刻画性质.

定理 6.3.1 对于一个实域 F, 下列叙述是等价的:

(1) F 是遗传欧氏域;

(2) F 没有次数可被 4 整除的有限扩张;

(3) F 的每个实有限扩张的扩张次数为奇数;

(4) $F(\sqrt{-1})$ 的每个代数扩张都是二次闭域;

(5) F 及其每个实代数扩张都只有惟一序;

(6) $F[x]$ 中每个不可约多项式在 F 的某个给定的实闭包中至多有一个根;

(7) 对于 F 的每个实代数扩张 K, K 的 F- 自同构必为恒等映射;

(8) 对于 F 的任意两个实闭包 R_1 和 R_2, R_1 和 R_2 是 $R_1 \cap R_2$- 同构的;

(9) 对于 F 的任意两个实闭包 R_1 和 R_2, $R_1^2 \cap R_2 = R_2^2 \cap R_1$, 即 R_1^2 和 R_2^2 在域 $R_1 \cap R_2$ 上诱导出相同的序.

证明 (1) $\Longrightarrow$ (2): 假若 F 有一个有限扩张 K, 使得扩张次数 $[K:F]$ 为 4 的倍数，则可进一步假定 K 是 F 的 Galois 扩张，且 $\sqrt{-1} \in K$. 设 H 是 Galois 群 $\mathrm{Aut}(K/F)$ 的 Sylow 2- 子群，则 $|H| \geqslant 4$. 令 E 为 H 的稳定子域，则由 Galois 基本定理知，$\mathrm{Aut}(K/E) = H$, 且 $[E:F] = [G:H]$. 此时，$[G:H]$ 为奇数. 由定理 1.3.4 的推论 1 可知，E 是 F 的实代数扩张. 由叙述 (1) 知，E 为欧氏域. 根据定理 6.2.3, $E(\sqrt{-1})$ 是一个二次闭域. 另一方面，$[K:E(\sqrt{-1})][E(\sqrt{-1}):E] = [K:E]$, 即 $[K:E(\sqrt{-1})] = \dfrac{1}{2}|H|$. 此外，显然 K 是 $E(\sqrt{-1})$ 的 Galois 扩张，且 $\dfrac{1}{2}|H|$ 是 2 的正指数方幂. 由 Galois 基本定理知，$E(\sqrt{-1})$ 有一个二次扩张，矛盾. 因而，叙述 (2) 成立.

(2) $\Longrightarrow$ (3): 假若 F 有一个偶次数的实扩张 K, 则 $\sqrt{-1} \notin K$. 从而 $K(\sqrt{-1})$ 是 F 的有限扩张，且 $[K(\sqrt{-1}):F]$ 为 4 的倍数，矛盾于叙述 (2).

(3) $\Longrightarrow$ (4): 设 K 是 $F(\sqrt{-1})$ 的任意代数扩张，且 R 是 F 的任意一个实闭包. 由于 $R(\sqrt{-1})$ 是 F 的代数闭包，从而可认定 $K \subseteq R(\sqrt{-1})$. 对于 $\alpha \in K$, 有 $\alpha = u + v\sqrt{-1}$, 且 $\sqrt{\alpha} = u_1 + v_1\sqrt{-1}$, 其中 $u, u_1, v, v_1 \in R$. 由本原元定理知，$F(u, u_1, v, v_1) = F(w)$. 设 w 在 $F(\sqrt{-1})$ 上的极小多项式为

$$g(x) = x^m + z_1 x^{m-1} + \cdots + z_m,$$

其中 $z_i = a_i + b_i\sqrt{-1}$, $a_i, b_i \in F$, $i = 1, \cdots, m$, 则有

$$(w^m + a_1 w^{m-1} + \cdots + a_m) + (b_1 w^{m-1} + \cdots + b_m)\sqrt{-1} = 0.$$

于是，w 是 F 上如下多项式的一个根

$$f(x) = x^m + a_1x^{m-1} + \cdots + a_m.$$

易知, $f(x)$ 在 F 上是不可约的. 因而, $[F(\sqrt{-1})(w) : F(\sqrt{-1})] = m = [F(w) : F]$. 由于 $F(w) \subseteq R$, 从而 $F(w)$ 是 F 的实代数扩张. 由叙述 (3) 知, m 为奇数. 假若 $\sqrt{\alpha} \notin F(\sqrt{-1})(\alpha)$, 则 $[F(\sqrt{-1})(\alpha, \sqrt{\alpha}) : F(\sqrt{-1})(\alpha)] = 2$. 注意到 $F(\sqrt{-1}, \alpha, \sqrt{\alpha}) \subseteq F(\sqrt{-1}, w)$, 从而

$$\begin{aligned} m &= [F(\sqrt{-1}, w) : F(\sqrt{-1})] \\ &= [F(\sqrt{-1}, w) : F(\sqrt{-1}, \alpha, \sqrt{\alpha})] \cdot [F(\sqrt{-1}, \alpha, \sqrt{\alpha}) : F(\sqrt{-1}, \alpha)] \\ &\quad \cdot [F(\sqrt{-1}, \alpha) : F(\sqrt{-1})] \end{aligned}$$

为偶数, 矛盾. 因此 $\sqrt{\alpha} \in F(\sqrt{-1})(\alpha)$. 由 α 的任意性知, K 是二次闭域.

(4) $\Longrightarrow$ (5): 设 K 是 F 的任意一个实代数扩张, 且 P 是 K 的任意正锥. 由叙述 (4) 知, $K(\sqrt{-1})$ 是二次闭域. 从而, 对于每个非零 $a \in P$, $\sqrt{a} \in K(\sqrt{-1})$, 即 $\sqrt{a} = c + d\sqrt{-1}$, 其中 $c, d \in K$. 由此有 $a^2 = c^2 - d^2 + 2cd\sqrt{-1}$. 于是 $cd = 0$. 如若 $c = 0$, 则 $a = -d^2 \in -P$, 矛盾. 从而 $d = 0$, 即 $a = c^2 \in K^2$. 于是 $P = K^2$. 因此, 叙述 (5) 成立.

(5) $\Longrightarrow$ (6): 如若不然, 则 $F[x]$ 中有某个不可约多项式 $f(x)$, 使得 $f(x)$ 在 R 中至少有两个相异根, 这里 R 是 F 的一个给定的实闭包. 设 α 是 $f(x)$ 在 R 中的一个根. 由定理 2.3.7 知, 正锥 $R^2 \cap F$ 在 $F(\alpha)$ 上至少有两个相异的拓展, 与叙述 (5) 矛盾. 因而叙述 (6) 成立.

(6) $\Longrightarrow$ (7): 令 R 是叙述 (6) 中给定的 F 的实闭包. 对于 $a \in R^2 \cap \dot{F}$, 有 $a = \alpha^2$, 其中 $\alpha \in \dot{R}$. 假若 $\alpha \notin F$, 则多项式 $x^2 - a$ 在 F 上不可约, 但它在 R 中有两个相异根 α 和 $-\alpha$; 这与叙述 (6) 矛盾. 从而 $\alpha \in F$. 于是有 $R^2 \cap F = F^2$. 因而, F^2 是 F 的惟一正锥.

设 K 是 F 的任意实代数扩张, 且 $\pi \in \mathrm{Aut}(K/F)$. 假若 π 不是 K 上的恒等映射, 则有 $\alpha \in K$, 使得 $\pi(\alpha) \neq \alpha$. 令 $f(x)$ 是 α 在 F 上的极小多项式, 且 $\beta = \pi(\alpha)$, 则显然 $f(\beta) = 0$. 由于 K 是一个实域, 从而 K 有一个实闭包 R_1. 注意到, R_1 和 R 都是序域 (F, F^2) 的实闭包. 由实闭包的惟一性知, 存在 R_1 到 R 的一个 F- 同构 τ. 此时有 $\tau(\alpha) \neq \tau(\beta)$, 但 $f(\tau(\alpha)) = f(\tau(\beta)) = 0$, 与叙述 (6) 矛盾. 从而叙述 (7) 成立.

(7) $\Longrightarrow$ (8): 令 $K = R_1 \cap R_2$, 且设 P 是 K 的任意一个正锥. 对于 $a \in P$, 由定理 1.3.4 的推论 2 知, $K(\sqrt{a})$ 是 K 的一个实扩张, 从而是 F 的实代数扩张. 假若 $\sqrt{a} \notin K$, 则有 $\pi \in \mathrm{Aut}(K(\sqrt{a})/K)$, 使得 $\pi(\sqrt{a}) = -\sqrt{a}$. 显然 $\pi \in \mathrm{Aut}(K(\sqrt{a})/F)$, 与叙述 (7) 矛盾. 从而 $\sqrt{a} \in K$, 即有 $a \in K^2$. 因此, K 仅有惟一的正锥 K^2. 于是 R_1 和 R_2 都是序域 (K, K^2) 的实闭包. 由实闭包的惟一性知, 叙述 (8) 成立.

(8) $\Longrightarrow$ (9): 令 $K = R_1 \cap R_2$. 由叙述 (8) 知, 存在 R_1 到 R_2 的一个 K- 同构 π.

设 $\alpha \in R_2^2 \cap R_1$, 则 $\alpha \in R_1$, 且 $\alpha \in R_2^2 = \pi(R_1)^2$. 从而有 $\beta \in R_1$, 使得 $\alpha = \pi(\beta)^2 = \pi(\beta^2)$. 注意到 $\alpha \in K$, 从而 $\pi(\alpha) = \alpha = \pi(\beta^2)$. 由此有 $\alpha = \beta^2 \in R_1^2 \cap R_2$. 因而, $R_2^2 \cap R_1 \subseteq R_1^2 \cap R_2$. 同理, $R_1^2 \cap R_2 \subseteq R_2^2 \cap R_1$. 因此, $R_1^2 \cap R_2 = R_2^2 \cap R_1$.

(9) $\Longrightarrow$ (1): 设 K 是 F 的任意一个实代数扩张, 且 P 为 K 的任意一个正锥. 假若 $P \neq K^2$, 则对于某个 $a \in P$, $a \notin K^2$. 由定理 2.3.8 的推论 2 知, $K(\sqrt{a})$ 有两个正锥 Q_1 和 Q_2, 使得 $\sqrt{a} \in Q_1$, 但 $-\sqrt{a} \in Q_2$. 令 R_i 是序域 $(K(\sqrt{a}), Q_i)$ 的实闭包, 其中 $i = 1, 2$. 此时, $\sqrt{a} \in R_1^2 \cap R_2$, 但 $-\sqrt{a} \in R_2^2 \cap R_1$. 于是 $R_1^2 \cap R_2 \neq R_2^2 \cap R_1$, 与叙述 (9) 矛盾. 因而, $P = K^2$, 即有 $K = K^2 \cup -K^2$. 这表明 K 是欧氏域. 因此 F 是遗传欧氏域. 证毕.

借助于 Galois 理论, W. D. Geyer 对遗传欧氏域给出了如下重要刻画.

定理 6.3.2 设 Ω 是域 F 的代数闭包, $G = \mathrm{Aut}(\Omega/F)$ 是 Ω 在 F 上的 Galois 群, 则 F 是遗传欧氏域, 当且仅当 $G = \langle\pi\rangle \cdot \Lambda$, 其中 π 的阶为 2, $\langle\pi\rangle$ 表示由 π 生成的循环群, Λ 是 G 的一个 Abel 子群, 使得 Λ 的稳定域是二次闭的, 且对于每个 $\lambda \in \Lambda$, $\pi\lambda\pi = \lambda^{-1}$.

证明 必要性: 设 F 为遗传欧氏域. 令 $\Lambda = \mathrm{Aut}\big(\Omega/F(\sqrt{-1})\big)$. 由于 $F(\sqrt{-1})$ 是 F 的正规扩张, 从而由无限 Galois 理论知, Λ 为 G 的正规子群, 且 $G/\Lambda \cong \mathrm{Aut}\big(F(\sqrt{-1})/F\big)$. 显然, $|\mathrm{Aut}\big(F(\sqrt{-1})/F\big)| = [F(\sqrt{-1}) : F] = 2$. 从而有 $[G : \Lambda] = 2$. 由于 F 是一个实域, 从而 F 在 Ω 中至少有一个实闭包 R. 此时, 由定理 2.1.3 知, $\Omega = R(\sqrt{-1})$. 从而有 $\pi \in \mathrm{Aut}(\Omega/R) \subseteq G$, 使得 $\pi(\sqrt{-1}) = -\sqrt{-1}$. 显然, π 的阶为 2, 且 $\pi \notin \Lambda$. 由刚才的论证知, $G = \langle\pi\rangle \cdot \Lambda$.

显然, Λ 的稳定域为 $F(\sqrt{-1})$. 由定理 6.3.1 知, $F(\sqrt{-1})$ 是二次闭域. 对于任意 $\alpha \in \Omega$, 总存在 F 的一个有限正规扩张 K, 使得 $\sqrt{-1}$, $\alpha \in K$. 对于每个 $\lambda \in \Lambda$, $\lambda|_K \in \mathrm{Aut}(K/F)$. 令 $H = \langle \lambda|_K \pi|_K \rangle$ 是由 $\lambda|_K \pi|_K$ 生成的 $\mathrm{Aut}(K/F)$ 的循环子群, 且记 L 为 H 的稳定子域. 注意到 $\lambda|_K \pi|_K (\sqrt{-1}) = -\sqrt{-1}$, 从而 $\sqrt{-1} \notin L$, 即 $[L(\sqrt{-1}) : L] = 2$. 此外, 由 Galois 基本定理知, $H = \mathrm{Aut}(K/L)$. 由于 $|H| = [K : L] = [K : L(\sqrt{-1})][L(\sqrt{-1}) : L] = 2[K : L(\sqrt{-1})]$, 从而 H 含有一个阶为 2 的子群 H_1. 令 L_1 为 H_1 的稳定子域. 由 Galois 基本定理知, L_1 是 L 的 Galois 扩张, $\mathrm{Aut}(L_1/L) \cong H/H_1$, 且 $[K : L_1] = |H_1| = 2$. 由定理 6.3.1 中叙述 (1) 和 (2) 的等价性知, $[K : F] = [K : L_1][L_1 : F] = 2[L_1 : F]$ 不被 4 整除, 即 $[L_1 : F]$ 是奇数. 因而 L_1 是 F 的一个实代数扩张. 再根据定理 6.3.1 中叙述 (1) 和 (7) 的等价性知, $|\mathrm{Aut}(L_1/L)| = 1$. 从而 $H = H_1$, 即 H 的阶为 2. 于是 $(\lambda|_K \pi|_K)^2$ 为 K 上的恒等映射, 即有 $(\lambda|_K \pi|_K)^2(\alpha) = \alpha$. 从而有 $(\lambda\pi)^2(\alpha) = \alpha$, 即 $\pi\lambda\pi(\alpha) = \lambda^{-1}(\alpha)$. 由 α 的任意性知, $\pi\lambda\pi = \lambda^{-1}$. 对于 $\lambda_1, \lambda_2 \in \Lambda$, $\pi(\lambda_1\lambda_2)\pi = (\lambda_1\lambda_2)^{-1} = \lambda_2^{-1}\lambda_1^{-1} = (\pi\lambda_2\pi)(\pi\lambda_1\pi) = \pi(\lambda_2\lambda_1)\pi$, 即有 $\lambda_1\lambda_2 = \lambda_2\lambda_1$. 因而, Λ 是 Abel 子群.

充分性：设 $G=\langle\pi\rangle\cdot\Lambda$, 其中 π 和 Λ 满足定理 6.3.2 中所示条件. 令 R 是子群 $<\pi>$ 的稳定域. 注意到，有限子群关于群 G 的 Krull 拓扑是闭的. 由无限 Galois 理论知， $\mathrm{Aut}(\Omega/R)=\langle\pi\rangle$, 即有 $[\Omega:R]=2$. 根据定理 2.2.1 知， R 是实闭域. 从而 F 是一个实域. 此时必有 $\pi(\sqrt{-1})=-\sqrt{-1}$. 记 E 是 Λ 的稳定域，则由所设知， E 是二次闭的. 从而 $\sqrt{-1}\in E$. 显然， $\Lambda\subseteq\mathrm{Aut}(\Omega/F(\sqrt{-1}))$, 但 $\pi\notin\mathrm{Aut}(\Omega/F(\sqrt{-1}))$. 因而，由 $G=<\pi>\cdot\Lambda$ 知，必定 $\Lambda=\mathrm{Aut}(\Omega/F(\sqrt{-1}))$. 此时， $\mathrm{Aut}(\Omega/F(\sqrt{-1}))\subseteq\mathrm{Aut}(\Omega/E)$, 即有 $E\subseteq F(\sqrt{-1})$. 于是， $F(\sqrt{-1})$ 是二次闭域.

假若 F 不是遗传欧氏域，则由定理 2.3.1 中叙述 (1) 和 (2) 的等价性知， F 有一个次数可被 4 整除的有限扩张 K. 显然，可进一步假定 $\sqrt{-1}\in K$, 且 K 是 F 的 Galois 扩张. 此时， $\mathrm{Aut}(K/F)=\langle\pi\mid_K\rangle\cdot\Lambda_K$, 这里 $\Lambda_K=\{\lambda\mid_K\mid\lambda\in\Lambda\}$. 由于 $|\langle\pi\mid_K\rangle|=2$, 且 $|\mathrm{Aut}(K/F)|=[K:F]$ 是 4 的倍数，从而 Λ_K 是 $\mathrm{Aut}(K/F)$ 的一个阶为偶数的子群. 由有限 Abel 群的结构知， Λ_K 可表为两个子群的直积 $\Lambda_K=H\times S$, 这里 S 是 Λ_K 的惟一的 Sylow 2- 子群， H 是 Λ_K 的一个阶为奇数的 (正规) 子群. 由条件知，对于每个 $h\in H$, $\pi\mid_K h\pi\mid_K^{-1}=h^{-1}\in H$. 由此易知， H 也是 $\mathrm{Aut}(K/F)$ 的一个正规子群. 令 L 是 H 的稳定子域. 由 Galois 基本定理知， L 是 F 的一个 Galois 扩张，且 $\mathrm{Aut}(L/F)\cong\mathrm{Aut}(K/F)/H\cong\langle\pi\mid_K\rangle\cdot S$. 由此可知， $\mathrm{Aut}(L/F)$ 是阶为 2^r 的群，其中 $r\geqslant 2$. 如若 $\sqrt{-1}\notin L$, 则 $|H|=[K:L]=[K:L(\sqrt{-1})][L(\sqrt{-1}):L]=2[K:L(\sqrt{-1})]$ 为偶数，矛盾. 从而 $\sqrt{-1}\in L$. 于是有 $[L:F(\sqrt{-1})]=2^{r-1}$. 再由 Galois 基本定理可知， $F(\sqrt{-1})$ 有一个二次扩张，矛盾. 因此， F 是一个遗传欧氏域. 证毕.

推论 若实域 F 有一个 Hensel 实赋值 v, 使得剩余域 F_v 是实闭域，且值群 G_v 是 2- 可除的，则 F 是遗传欧氏域.

证明 由定理 6.3.1 知，只需证明 F 的每个实代数扩张只有惟一序. 设 K 是 F 的任意实代数扩张，则 K 至少有一个正锥 Q. 由定理 3.4.5, v 与 $Q\cap F$ 相容. 根据定理 3.2.4, v 可以拓展为 K 的一个实赋值 w. 由 Hensel 赋值的定义可知， w 也是 K 的一个 Hensel 赋值. 再由定理 3.4.5 知， $\mathcal{X}_K=\mathcal{X}_K^w$. 注意到 F_w 是 F_v 的代数扩张，且 F_w 为实域. 由于 F_v 是实闭域，从而 $F_w=F_v$ 是实闭域. 设 $\lambda\in G_w$, 则由关于赋值域的代数扩张的熟知事实知，有自然数 m, 使得 $m\lambda\in G_v$. 令 $m=2^k(2n+1)$, 其中 n 和 k 为非负整数. 由于 G_v 是 2- 可除的，从而有 $g\in G_v$, 使得 $2^{k+1}g=2^k(2n+1)\lambda$, 即 $2g=(2n+1)\lambda$. 由此有 $\lambda=2(g-n\lambda)\in 2G_w$. 因而， $G_w=2G_w$, 即 $|G_w/2G_w|=1$. 显然， $|\mathcal{X}_{F_w}|=1$. 根据定理 5.6.7 的推论 1 知， $|\mathcal{X}_K|=|\mathcal{X}_K^w|=1$, 即 K 仅有惟一序. 证毕.

通过上面推论，我们容易给出下面的一个例子，这个例子表明：遗传欧氏域不一定是实闭域.

例 设 G 是有理数加法群 $(\mathbb{Q},+)$ 的如下子群:

$$G=\left\{\frac{m}{2^n}\mid m,n\in\mathbb{Z},且n\geqslant 0\right\}.$$

显然, G 是 2- 可除的, 且对于有理数之间的通常大小关系是一个序群.

按照 §5.7 中例 2, 令 $F=\mathbb{R}((G))$ 是系数在实数域 $\mathbb{R}$ 中而指数在 G 中的形式幂级数域, 且 v 为域 F 的自然赋值, 则 $F_v\cong\mathbb{R}$, 且 $G_v=G$. 因而, F_v 是实闭域, 且 G_v 是 2- 可除的.

此外, 作为赋值论的一个熟知事实, v 是域 F 的一个 Hensel 赋值. 因此, 由上面推论知, F 是一个遗传欧氏域. 然而, 易知奇次数多项式 x^3-t 在 F 中没有解, 这里 t 为 G 到 $\mathbb{R}$ 的这样一个映射, 使得 $\mathrm{supp}(t)=\{1\}$, 且 $t(1)=1$. 因此, F 不是实闭域.

遗传欧氏域与 SAP 域之间具有某种联系, 这种联系可由下面定理看出.

定理 6.3.3 一个实域 F 是遗传欧氏域, 当且仅当 $F(x)$ 的每个实代数扩张是 SAP 域, 这里 x 是域 F 上一个未定元.

证明 设 $F(x)$ 是一个 SAP 域. 令 $K=F(\alpha)$ 是 F 的任意实有限扩张, 且 α 在 F 上的极小多项式为 $f(x)$. 由命题 3.1.1(1) 知, $F(x)$ 有一个赋值 v, 使得 $G_v=\mathbb{Z}$, 且 $F_v\cong F(\alpha)$. 由于 K 是实域, 从而 v 是一个实赋值. 由于 $|G_v/2G_v|=2$, 从而由定理 6.1.2 知, $|\mathcal{X}_{F_v}|=1$. 这表明, K 仅有惟一序. 由定理 6.3.1 知, F 为遗传欧氏域.

现设 F 为遗传欧氏域. 令 L 是 $F(x)$ 的任意实有限扩张, 且 v 是 L 的一个实赋值. 令 v_0 是 v 在 F 上的限制. 由于 F 为欧氏域, 从而 v_0 的值群 G_{v_0} 显然是 2- 可除的. 下面分情况证明: $|G_v/2G_v|\leqslant 2$, 且当 $|G_v/2G_v|=2$ 时, $|\mathcal{X}_{F_v}|=1$.

情况 1 G_v 包含在 G_{v_0} 的可除闭包中. 此时易知, G_v 也是 2- 可除的, 此正为欲证.

情况 2 G_v 不包含在 G_{v_0} 的可除闭包中. 此时, 有 $z\in L$, 使得对于任意整数 k, $kv(z)\notin G_{v_0}$, 即 $v(z^k)\notin G_{v_0}$. 令 v_1 是赋值 v 在域 $F(z)$ 上的限制, 则对于相异的整数 m,n 以及任意 $a,b\in\dot{F}$, $v_1(az^m)\neq v_1(bz^n)$. 因而, 对于 $\sum\limits_{i=0}^{n}a_iz^i\in F(z)$, 有

$$v_1\left(\sum_{i=0}^{n}a_iz^i\right)=\min\{v_0(a_i)+iv(z)\mid i=0,1,\cdots,n\}\in G_{v_0}+\mathbb{Z}\cdot v(z).$$

由此可见, $G_{v_1}\cong G_{v_0}\oplus\mathbb{Z}$. 设 $\alpha\in A_{v_1}\setminus M_{v_1}$. 由 $F(z)$ 中元素的形式, 可令 $\alpha=\left(\sum\limits_{i=0}^{n}a_iz^i\right)\left(\sum\limits_{i=0}^{n}b_iz^i\right)^{-1}$, 其中 $a_i,b_i\in F$, $i=0,\cdots,n$. 于是, $v_1\left(\sum\limits_{i=0}^{n}a_iz^i\right)=$

$v_1\left(\sum_{i=0}^{n} b_i z^i\right)$. 令 $v_1(a_k z^k) = \min\{v_1(a_i z^i) \mid i = 0, \cdots, n\}$, $0 \leqslant k \leqslant n$, 则必有 $v_1(b_k z^k) = \min\{v_1(b_i z^i) \mid i = 0, \cdots, m\}$. 由此知 $v_1(a_k) = v_1(b_k)$, 即 $a_k b_k^{-1} \in A_{v_1} \setminus M_{v_1}$. 此时, $\alpha - a_k b_k^{-1} = \left[\sum_{i\neq k}(b_k a_i - a_k b_i)z^i\right]\left(\sum_{i=0}^{n} b_k b_i z^i\right)^{-1}$. 对于不等于 k 的每个 i, $v_1((b_k a_i - a_k b_i)z^i) \geqslant \min\{v_1(b_k a_i z^i), v_1(a_k b_i z^i)\} = v_1(b_k) + \min\{v_1(a_i z^i), v_1(b_i z^i)\} > v_1(b_k) + v_1(b_k z^k) = v_1\left(\sum_{i=0}^{n} b_k b_i z^i\right)$. 从而有 $\alpha - a_k b_k^{-1} \in M_{v_1}$, 即 $\alpha + M_{v_1} = a_k b_k^{-1} + M_{v_1}$. 因而 $F_{v_1} = F_{v_0}$. 显然, z 是 F 上超越元. 从而 L 是 $F(z)$ 的有限扩张. 于是, $[G_v : G_{v_0} \oplus \mathbb{Z}]$ 和 $[F_v : F_{v_0}]$ 都是有限的. 据此, 我们可以证明如下两个事实.

事实 1　$|G_v/2G_v| = 2$.

设 $[G_v : G_{v_0} \oplus \mathbb{Z}] = r$, 则有自然数 s, 使得 $2^s > r$. 假若 $1 \in 2^s G_v$, 则 $r = r \cdot 1 \in 2^s(rG_v) \subseteq 2^s(G_{v_0} \oplus \mathbb{Z})$, 即 $r = 2^s\xi + 2^s k$, 其中 $\xi \in G_{v_0}$, $k \in \mathbb{Z}$. 从而有 $r = 2^s k$, 矛盾. 因而, $1 \notin 2^s G_v$. 然而, $1 \in 2^0 G_v$. 从而有一个最大非负整数 m, 使得 $1 \in 2^m G_v$, 即 $\frac{1}{2^m} \in G_v$. 对于任意 $g \in G_v$, 有自然数 k, 使得 $kg \in G_{v_0} \oplus \mathbb{Z} \subseteq G_{v_0} \oplus \mathbb{Z} \cdot \frac{1}{2^m}$, 即 $kg = \eta + \frac{t}{2^m}$, 其中 $\eta \in G_{v_0}$, $t \in \mathbb{Z}$. 此外, 可选取 k 尽可能小. 假若 k 为偶数, 则当 $t = 2t_1$ 为偶数时, $\frac{k}{2}g = \frac{\eta}{2} + \frac{t_1}{2^m} \in G_{v_0} \oplus \mathbb{Z} \cdot \frac{1}{2^m}$, 与 k 的选取矛盾. 当 $t = 2t_1 + 1$ 为奇数时, $\frac{1}{2^m} = 2\left(\frac{k}{2}g - \frac{t_1}{2^m} + \frac{\eta}{2}\right) \in 2G_v$, 即有 $1 \in 2^{m+1}G_v$, 与 m 的最大性矛盾. 因而, k 为奇数, 即 $k = 2k_1 + 1$, 其中 $k_1 \geqslant 0$. 由此有 $g = \frac{t}{2^m} + \eta - 2k_1 g$. 当 $t = 2t_1$ 为偶数时, $g \in 2G_v$; 而当 $t = 2t_1 + 1$ 为奇数时, $g - \frac{1}{2^m} \in 2G_v$, 即 $g \in \frac{1}{2^m} + 2G_v$. 因而, $G_v = 2G_v \cup \left(\frac{1}{2^m} + 2G_v\right)$. 由 m 的最大性可知, $\frac{1}{2^m} \notin 2G_v$. 因此, $|G_v/2G_v| = 2$.

事实 2　剩余域 F_v 仅有惟一序.

设 $F_v = F_{v_0}(\bar{\alpha})$, 且 $\bar{f}(y)$ 是 $\bar{\alpha}$ 在 F_{v_0} 上的极小多项式, 则 $A_{v_0}[y]$ 中有一个首项系数为 1 的多项式 $f(y)$, 使得在典型同态: $A_{v_0}[y] \longrightarrow F_{v_0}[y]$ 下, $f(y)$ 的像恰为 $\bar{f}(y)$. 显然, $f(y)$ 在域 F 上是不可约的. 令 β 是 $f(y)$ 在 F 的代数闭包中一个根, 且 w 是赋值 v_0 在 $F(\beta)$ 上的一个拓展. 由 $f(\beta) = 0$ 知, β 在 A_{v_0} 上整. 从而 $\beta \in A_w$, 即有 $\bar{\beta} = \beta + M_w \in F_w$. 显然, $\bar{\beta}$ 是 $\bar{f}(y)$ 的一个根. 于是 $[F_{v_0}(\bar{\beta}) : F_{v_0}] = \deg\bar{f}(y)$. 注意到 $F_{v_0}(\bar{\beta}) \subseteq F_w$, 且 $[F_w : F_{v_0}] \leqslant [F(\beta) : F] = \deg f(y) = \deg\bar{f}(y)$. 因而有 $F_w = F_{v_0}(\bar{\beta})$. 由于 $\bar{\alpha}$ 和 $\bar{\beta}$ 都是域 F_{v_0} 上不可约多项式 $\bar{f}(y)$ 的根, 从而 $F_w \cong F_{v_0}(\bar{\alpha}) = F_v$. 由此可见, w 是 $F(\beta)$ 的一个实赋值, 且 $F(\beta)$ 是 F 的一个实有限扩张. 由定理 6.3.1 知, $F(\beta)$ 仅有惟一序 P. 自然有 $\mathcal{X}^w_{F(\beta)} = \{P\}$. 根据定理 5.6.7 的推论 1 知, $|\mathcal{X}_{F_w}| = 1$,

即 $|\mathcal{X}_{F_v}|=1$.

根据定理 6.1.2, 上面两个事实表明： L 是一个 SAP 域. 证毕.

实际上，定理 6.3.3 可得到进一步改进. 在此之前，我们需要一些预备工作.

设 F 是一个域， P 是 F 的一个正锥，且 R 是序域 (F,P) 的实闭包. 对于 $\alpha\in R$, 设 $f_\alpha(x)$ 是 α 在 F 上的极小多项式. 由命题 3.1.3(1), 有理函数域 $F(x)$ 有一个赋值 v, 使得下列条件成立： (1) 对于每个非零 $a\in F$, $v(a)=0$; (2)$v(f_\alpha(x))=1$; (3) 且剩余域 $F_v\cong F[x]/\big(f_\alpha(x)\big)\cong F(\alpha)$. 在下文中，这样一个赋值 v 将记作 v_α. 显然， v_α 是 $F(x)$ 的一个非浅显的实赋值.

引理 6.3.4 设 K 是有理函数域 $F(x)$ 的一个有限扩张， Q 为 K 的一个正锥，且 R 是序域 $(F,Q\cap P)$ 的实闭包，则存在 R 中一个开区间 $]a,b[_{R^2}$, 使得对于每个 $\alpha\in]a,b[_{R^2}$, v_α 可拓展为 K 的一个实赋值.

证明 由定理 3.6.9 知, 存在 R 中一个开区间 $]a,b[_{R^2}$, 使得对于每个 $\alpha\in]a,b[_{R^2}$, 总有一个 F- 位 ϕ: $K\longrightarrow R\cup\{\infty\}$, 使得 $\phi(x)=\alpha$. 令 w 是与位 ϕ 相对应的赋值. 由于 ϕ 是实位，从而 w 是 K 的一个实赋值. 不难验证： w 是 v_α 在 K 上的一个拓展. 证毕.

引理 6.3.5 设 K 是域 F 的一个有限扩张，且 F 有一个正锥 P, 使得 P 在 K 上有惟一拓展，则 F 的每个正锥都可拓展为 K 的一个正锥. 特别地，若 K 仅有惟一序，则 F 也仅有惟一序.

证明 设 R 是序域 (F,P) 的实闭包. 由所设，令 $K=F(\alpha)$, 且 $f(x)$ 是 α 在 F 上的极小多项式. 由于 P 在 K 上仅有惟一拓展，从而由定理 2.3.8 知， $f(x)$ 在 R 中仅有一个根. 这表明： $f(x)$ 的次数是奇数，即 K 是 F 的一个奇次数扩张. 根据定理 1.3.4 的推论 1, F 的每个正锥都可拓展为 K 的正锥.

若 K 仅有惟一正锥 Q, 则 $Q\cap F$ 是 F 的一个正锥，且 $Q\cap F$ 在 K 上有惟一拓展 Q. 对于 F 的任意正锥 P, 由上面的结果知， P 在 K 上有一个拓展. 由所设知， P 在 K 上的这个拓展只能为 Q. 因而， $P=Q\cap F$. 证毕.

现在，我们可以建立下面定理，这个定理是定理 6.3.3 的一个改善.

定理 6.3.6 设 K 是域 F 上有理函数域 $F(x)$ 的一个实有限扩张，则 F 是遗传欧氏域，当且仅当 K 是 SAP 域.

证明 由定理 6.3.3 知，只须证明充分性. 设 K 是一个 SAP 域. 令 R 是序域 $(F,Q\cap F)$ 的实闭包，这里 Q 为 K 的一个正锥. 假若 F 不是遗传欧氏域，则由定理 6.3.1 知，在 R 中， F 的某个实有限扩张 $F(\beta)$ 至少有两个相异的正锥. 由引理 6.3.4 知， R 有一个开区间 $]a-\epsilon,a+\epsilon[_{R^2}$, 其中 $\epsilon\in F$, 且 $\epsilon>_{R^2}0$, 使得对于每个 $\alpha\in]a-\epsilon,a+\epsilon[_{R^2}$, v_α 可拓展为 K 的一个实赋值.

任意取出 $\alpha\in]a-\epsilon,a+\epsilon[_{R^2}$. 由本原元定理知， $F(\beta,\alpha)=F(\theta)$, 其中 $\theta\in R$,

且 $\theta >_{R^2} 0$. 由于 $F(\beta)$ 至少有两个正锥，从而由引理 6.3.5 知，$F(\theta)$ 至少有两个正锥. 对于每个自然数 n, 令 $\alpha_n = \alpha + \dfrac{\epsilon}{n(1+\theta)}$, 则显然 $F \subseteq F(\alpha_n) \subseteq F(\theta)$. 由于 F 和 $F(\theta)$ 只有有限个中间域，从而有相异的自然数 r 和 s, 使得 $F(\alpha_r) = F(\alpha_s)$. 此时可知 $\theta \in F(\alpha_r)$, 即 $F(\alpha_r) = F(\theta)$. 显然 $\alpha_r \in]a-\epsilon, a+\epsilon[_{R^2}$, 从而 v_{α_r} 可拓展为 K 的一个实赋值 w. 由于 v_{α_r} 的剩余域为 $F(\alpha_r) = F(\theta)$, 且 w 的剩余域 F_w 是 $F(\theta)$ 的实有限扩张，从而由引理 6.3.5 知，$|\mathcal{X}_{F_w}| \neq 1$. 此外，商群 G_w/H 是有限阶的，且 $H \cong \mathbb{Z}$, 这里 H 是 F 的赋值 v_{α_r} 的值群. 从而易知，G_w 不是 2- 可除的. 因而 $|G_w/2G_w| \geqslant 2$. 根据定理 6.1.2 知，K 不是 SAP 域，与所设矛盾. 因此，F 是一个遗传欧氏域. 证毕.

作为上面定理的一个推论，我们可建立如下重要结果.

定理 6.3.7 设 F 是一个实函数域，K 是 F 的一个实有限扩张，则 F 是 SAP 域，当且仅当 K 是 SAP 域.

证明 由函数域的定义可知，存在 F 的一个子域 F_0, 使得 F 是 $F_0(x)$ 的有限扩张，其中 $x \in F$ 是 F_0 上的一个超越元. 由定理 6.3.6 知，F 是 SAP 域 $\Longleftrightarrow F_0$ 为遗传欧氏域 $\Longleftrightarrow K$ 为 SAP 域. 证毕.

§6.4 序空间同胚于指定的 Bool 空间的实域

在 §1.5 中，我们证明了这样一个重要事实：每个实域的序空间对于 Harrison 拓扑是一个全不连通的 Hausdorff 紧空间. 在拓扑学中，一个全不连通的 Hausdorff 紧空间也称作 Bool 空间. 自然会问：对于事先指定的一个 Bool 空间 $\mathcal{B}$, 是否总有一个实域 F, 使得 $\mathcal{X}_F$ 同胚于 $\mathcal{B}$? 对于这一问题，T. C. Craven 给出了肯定的回答. 在本节中，我们将沿着 Craven 的论证过程，对上面问题加以讨论. 首先，我们需要如下关于全不连通的 Hausdorff 紧空间的拓扑性质.

命题 6.4.1 设 $\mathcal{X}$ 是一个 Bool 空间，则

(1) $\mathcal{X}$ 的所有既开又闭的子集组成一个基;

(2) $\mathcal{X}$ 同胚于某个乘积拓扑空间 $\{1,-1\}^{\mathcal{B}}$ 的一个闭子集，这里集合 $\{1,-1\}$ 被赋予离散拓扑.

证明 (1) 对于任意 $x \in \mathcal{X}$, 用 $C(x)$ 表示所有包含 x 的既开又闭子集的交. 显然, $C(x)$ 是 $\mathcal{X}$ 的闭子集. 假若 $C(x) \neq \{x\}$, 则由 $\mathcal{X}$ 的全不连通性有，$C(x) = F_1 \cup F_2$, 其中 F_1 和 F_2 是 $\mathcal{X}$ 的两个不相交的非空闭子集. 不妨设 $x \in F_1$. 由于 $\mathcal{X}$ 是 Hausdorff 紧空间，从而由拓扑知识知，有某个开子集 D, 使得 $F_1 \subseteq D$, 但 $\bar{D} \cap F_2 = \phi$, 其中 $\bar{D}$ 表示 D 的闭包. 令 $C = \bar{D} \cap (\mathcal{X} \setminus D)$ 为 D 的边界. 注意到 $\bar{D} \cap F_2 = (\mathcal{X} \setminus D) \cap F_1 = \phi$, 从而 $C \cap C(x) = \phi$. 于是对于每个 $y \in C$, 存在一个包含 x 的既开又闭子集 H_y, 使

得 $y \notin H_y$. 从而得到 C 的这样一个开复盖 $C \subseteq \bigcup_{y \in C}(\mathcal{X} \setminus H_y)$. 由于 C 是紧空间 $\mathcal{X}$ 的闭子集，从而有一个有限开复盖 $C \subseteq \bigcup_{i=1}^{n}(\mathcal{X} \setminus H_{y_i})$, 其中 $y_i \in C$, $i = 1, \cdots, n$. 令 $H = \bigcap_{i=1}^{n} H_{y_i}$, 且 $W = D \cap H$. 显然， $W = (D \cup C) \cap H = \bar{D} \cap H$. 因此，$W$ 是既开又闭的. 注意到 $x \in W$. 由 $C(x)$ 的规定知， $F_2 \subseteq C(x) \subseteq W$. 然而 $F_2 \cap W \subseteq F_2 \cap D = \phi$, 矛盾. 因而，对于每个 $x \in \mathcal{X}$, $C(x) = \{x\}$.

现设 U 是 $\mathcal{X}$ 中任意点 x 的一个开邻域，则 $\mathcal{X} \setminus U$ 是 $\mathcal{X}$ 的闭子集. 对于任意 $y \in \mathcal{X} \setminus U$, 由上面讨论知， $x \notin C(y)$. 从而有一个包含 y 的既开又闭子集 H_y, 使得 $x \notin H_y$. 由开复盖 $\mathcal{X} \setminus U \subseteq \bigcup_{y \in \mathcal{X} \setminus U} H_y$, 可得一个有限开复盖 $\mathcal{X} \setminus U \subseteq \bigcup_{i=1}^{n} H_{y_i}$, 其中 $y_i \in \mathcal{X} \setminus U$, $i = 1, \cdots, n$. 令 $H = \bigcap_{i=1}^{n}(\mathcal{X} \setminus H_{y_i})$, 则 H 是 $\mathcal{X}$ 的既开又闭子集，使得 $x \in H \subseteq U$. 这表明 $\mathcal{X}$ 的所有既开又闭的子集组成一个基.

(2) 由结论 (1) 知，$\mathcal{X}$ 有一个基 $\mathcal{B}$, 其中 $\mathcal{B}$ 由 $\mathcal{X}$ 的所有既开又闭的子集组成.

对于 $\mathcal{X}$ 的任意子集 H, 用 λ_H 表示 $\mathcal{X}$ 上由 H 所确定的特征函数，即对于 $x \in \mathcal{X}$, 若 $x \in H$, $\lambda_H(x) = 1$; 否则， $\lambda_H(x) = -1$. 这样，对于每个 $x \in \mathcal{X}$, 可规定 $\mathcal{B}$ 到 $\{1, -1\}$ 的如下一个映射：

$$\hat{x}:\ B \longmapsto \lambda_B(x), \quad B \in \mathcal{B}.$$

据此，我们可得到 $\mathcal{X}$ 到 $\{1, -1\}^{\mathcal{B}}$ 的如下映射：

$$\phi:\ x \longmapsto \hat{x}, \qquad x \in \mathcal{X}.$$

由于 $\mathcal{X}$ 是 Hausdorff 的，从而 ϕ 显然是单射. 由乘积拓扑的定义知， $\{1, -1\}^{\mathcal{B}}$ 的一个子基由如下子集组成：

$$H_B^{\lambda} = \{f \in \{1, -1\}^{\mathcal{B}} \mid f(B) = \lambda\},$$

其中 $B \in \mathcal{B}$, $\lambda = \pm 1$.

显然， $\phi^{-1}(H_B^1) = B$, 而 $\phi^{-1}(H_B^{-1}) = \mathcal{X} \setminus B$. 因此， $\mathcal{X}$ 同胚于 $\{1, -1\}^{\mathcal{B}}$ 的子空间 $\phi(\mathcal{X})$.

设 $f \in \{1, -1\}^{\mathcal{B}}$, 但 $f \notin \phi(\mathcal{X})$, 则有如下两种可能情况.

情况 1 对于某个 $B \in \mathcal{B}$, $f(B) = f(\mathcal{X} \setminus B) = \lambda$, 其中 $\lambda = \pm 1$. 此时，$f \in H_B^{\lambda} \cap H_{\mathcal{X} \setminus B}^{\lambda}$, 且显然 $H_B^{\lambda} \cap H_{\mathcal{X} \setminus B}^{\lambda} \cap \phi(\mathcal{X}) = \phi$.

情况 2 对于每个 $B \in \mathcal{B}$, $f(B) \neq f(\mathcal{X} \setminus B)$. 由于 $f \notin \phi(\mathcal{X})$, 从而对于每个 $x \in \mathcal{X}$, $f \neq \hat{x}$. 于是有某个 $B_x \in \mathcal{B}$, 使得 $f(B_x) \neq \hat{x}(B_x)$. 由此必有 $f(\mathcal{X} \setminus B_x) \neq \hat{x}(\mathcal{X} \setminus B_x)$; 否则 $f(\mathcal{X} \setminus B_x) = \hat{x}(\mathcal{X} \setminus B_x) \neq \hat{x}(B_x)$, 即 $f(\mathcal{X} \setminus B_x) = f(B_x)$, 矛盾. 必

要时，可将 $\mathcal{X}\setminus B_x$ 代替 B_x, 从而可设 $\hat{x}(B_x)=1$, 即 $x\in B_x$. 因而，我们有一个开复盖：$\mathcal{X}\subseteq\bigcup\limits_{x\in\mathcal{X}}B_x$. 由 $\mathcal{X}$ 的紧性知，有这样一个有限开复盖：$\mathcal{X}=\bigcup\limits_{i=1}^{n}B_{x_i}$, 其中 $x_i\in\mathcal{X}$, $i=1,\cdots,n$. 此时易知 $f\in\bigcap\limits_{i=1}^{n}H_{B_{x_i}}^{-1}$, 但 $\left(\bigcap\limits_{i=1}^{n}H_{B_{x_i}}^{-1}\right)\cap\phi(\mathcal{X})=\phi$.

由上面的讨论即知，$\phi(\mathcal{X})$ 是拓扑空间 $\{1,-1\}^{\mathcal{B}}$ 的闭子集. 证毕.

设 F 是任意域，Ω 是 F 的代数闭包. 对于 F 的任意子集 A, 记 $\sqrt{A}=\{\alpha\in\Omega\mid\alpha^2\in A\}$. $\sqrt{A}$ 的一个子集 B 称作 A 在 F 上的一个平方根基，如果下列条件成立：(1)$\sqrt{A}\subseteq F(B)$; (2) 对于任意有限个相异的 $b_1,\cdots,b_n\in B$, 扩张次数 $[F(b_1,\cdots,b_n):F]=2^n$; 等价于：对于每个 $b\in B$, $b\notin F(B\setminus\{b\})$.

引理 6.4.2 (1) 所设同上, 则 F 的每个子集 A 都有一个在 F 上的平方根基.

(2) 进一步设 F 是一个实域，$A\subseteq F$, 且 B 是 A 在 F 上的一个平方根基，则 $\bigcap\limits_{a\in A}H(a)$ 中每个正锥都可惟一地拓展为 $F(B)$ 的一个包含 B 的正锥.

证明 (1) 考察如下集合

$$\Xi=\{C\mid C\subseteq\sqrt{A},\text{且对于每个 }c\in C, c\notin F(C\setminus\{c\})\}.$$

显然 $\phi\in\Xi$, 且 Ξ 对于集合的包含关系是一个偏序集. 由 Zorn 引理可知，Ξ 中有一个极大成员 B. 设 $\alpha\in\sqrt{A}$. 假若 $\alpha\notin F(B)$, 则自然 $\alpha\notin B$. 令 $C=B\cup\{\alpha\}$. 由 B 在 Ξ 中的极大性知，$C\notin\Xi$. 于是有有限个相异的元素 $c_1,\cdots,c_n\in C$, 使得 $[F(c_1,\cdots,c_n):F]<2^n$. 由于 $B\in\Xi$, 从而必有 $\alpha\in\{c_1,\cdots,c_n\}$. 因而可令 $c_n=\alpha$, 而 $c_i\in B$, $i=1,\cdots,n-1$. 此时，显然有 $[F(c_1,\cdots,c_{n-1}):F]=2^{n-1}$. 注意到 $[F(c_1,\cdots,c_{n-1})(\alpha):F(c_1,\cdots,c_{n-1})][F(c_1,\cdots,c_{n-1}):F]=[F(c_1,\cdots,c_{n-1},c_n):F]<2^n$. 从而 $[F(c_1,\cdots,c_{n-1})(\alpha):F(c_1,\cdots,c_{n-1})]<2$, 即有 $\alpha\in F(c_1,\cdots,c_{n-1})\subseteq F(B)$, 矛盾. 从而，$\alpha\in F(B)$. 因此，$B$ 是 A 在 F 上的一个平方根基.

(2) 设 $P\in\bigcap\limits_{a\in A}H(a)$. 考察如下集合：

$$\Sigma=\{C\mid C\subseteq B,\text{且 }P\text{ 可拓展为 }F(C)\text{ 的一个正锥 }Q,\text{使得 }C\subseteq Q\}.$$

显然 $\phi\in\Sigma$, 且 Σ 对于集合的包含关系是一个偏序集.

此时可断言：若 $C_1,C_2\in\Sigma$, 其中 $C_1\subseteq C_2$, Q_1,Q_2 分别为 P 在 $F(C_1),F(C_2)$ 上所拓展的正锥，且 $C_1\subseteq Q_1$, $C_2\subseteq Q_2$, 则 $Q_1\subseteq Q_2$, 即 $Q_2\cap F(C_1)=Q_1$.

事实上，如若 $Q_1\neq Q_2\cap F(C_1)$, 则 C_1 中有有限个元素 $c_1,\cdots,c_m$, 使得 $Q_1\cap F(c_1,\cdots,c_m)\neq Q_2\cap F(c_1,\cdots,c_m)$. 选取最小自然数 m, 使得这样的不等式成立. 从而有 $Q_1\cap F(c_1,\cdots,c_{m-1})=Q_2\cap F(c_1,\cdots,c_{m-1})$. 令 $Q'=Q_1\cap F(c_1,\cdots,c_{m-1})$, 则 Q' 是域 $F(c_1,\cdots,c_{m-1})$ 的一个正锥. 注意到 $c_m^2\in A\subseteq P\subseteq Q'$. 由定理 2.3.8 的推论

2 知, Q' 在 $F(c_1,\cdots,c_{m-1},c_m)$ 上恰有两个拓展, 使得 c_m 关于这两个拓展分别为正和负元素. 显然 $Q_1\cap F(c_1,\cdots,c_m)$ 和 $Q_2\cap F(c_1,\cdots,c_m)$ 都是 Q' 在域 $F(c_1,\cdots,c_m)$ 上的拓展, 而且 c_m 对于这两个拓展都为正元素. 从而有 $Q_1\cap F(c_1,\cdots,c_m) = Q_2\cap F(c_1,\cdots,c_m)$, 矛盾. 因此, 上面的断言成立.

设 $\{C_i \mid i\in I\}$ 是 Σ 中任意一个链, 其中 I 是一个指标集. 对于每个 $i\in I$, P 可拓展为 $F(C_i)$ 的一个正锥 Q_i, 使得 $C_i\subseteq Q_i$. 由上面的断言知, 当 $C_i\subseteq C_j$ 时, 其中 $i,j\in I$, 总有 $Q_i\subseteq Q_j$.

令 $C=\bigcup\limits_{i\in I}C_i$, 且 $Q=\bigcup\limits_{i\in I}Q_i$. 由上面的讨论, 易知 Q 是 P 在域 $F(C)$ 上所拓展的一个正锥, 且 $C\subseteq Q$. 从而 $C\in\Sigma$. 因而, 链 $\{C_i\mid i\in I\}$ 在 Σ 中有一个上界 C. 由 Zorn 引理, Σ 中有一个极大元 B_0.

假若 $B_0\neq B$, 则有 $b\in B$, 使得 $b\notin B_0$. 此时, 显然 $b\notin F(B_0)$. 由于 $B_0\in\Sigma$, 从而 P 在 $F(B_0)$ 上有一个拓展 Q_0, 使得 $B_0\subseteq Q_0$. 由定理 2.3.8 的推论 2 知, Q_0 在 $F(B_0)(b)$ 上有一个拓展 Q_1, 使得 $b\in Q_1$. 这表明 $B_0\cup\{b\}\in\Sigma$, 矛盾于 B_0 的极大性. 因此, $B_0=B$. 这表明: P 可拓展为 $F(B)$ 的一个正锥 Q, 使得 $B\subseteq Q$.

再设 Q_1, Q_2 都是 P 在域 $F(B)$ 上的拓展, 且 $B\subseteq Q_i$, $i=1,2$. 由上面的断言知, $Q_1=Q_2$. 引理获证. 证毕.

定理 6.4.3 设 F 是一个 SAP 域, 且 C 是 $\mathcal{X}_F$ 的一个闭子集, 则 F 有一个代数扩张 K: 使得限制映射 $r: Q\longmapsto Q\cap F$ 是 $\mathcal{X}_K$ 到 C 的一个同胚.

证明 当 $C=\mathcal{X}_F$ 时, 取 $K=F$ 即可. 下设 $C\neq\mathcal{X}_F$. 由命题 6.1.1 知, $\mathcal{H}=\{H(a)\mid a\in\dot{F}\}$ 是序空间 $\mathcal{X}_F$ 的一个基. 由所设知, $\mathcal{X}_F\setminus C$ 是 $\mathcal{X}_F$ 的一个开子集, 即有 $\mathcal{X}_F\setminus C=\bigcup\limits_{b\in B}H(b)$, 这里 B 是 F 的一个非空子集, 使得对于每个 $b\in B$, $H(b)\neq\emptyset$. 从而 $C=\bigcap\limits_{a\in A}H(a)$, 其中 $A=-B$.

对于每个非负整数 n, 我们可以归纳地定义这样的一个偶 (K_n,A_n), 使得下列条件成立:

(1) $K_0=F$, 且 $A_0=A$;

(2) 当 (K_n,A_n) 被确定时, A_{n+1} 为 A_n 在 K_n 上的一个平方根基, 且 $K_{n+1}=K_n(A_{n+1})$.

显然 $K_n\subseteq K_{n+1}$, $n=0,1,\cdots$. 令 $K=\bigcup\limits_{n=0}^{\infty}K_n$, 则 K 是 F 的一个代数扩张. 下面证明: 由此所得的扩张 K 满足定理中所要求的条件.

对于任意 $P\in C$, 由引理 6.4.2 知, P 可拓展为 K_1 的一个正锥 Q_1, 使得 $A_1\subseteq Q_1$. 再由引理 6.4.3, Q_1 可进一步拓展为 K_2 的一个正锥 Q_2, 使得 $A_2\subseteq Q_2$. 一般地, 对于 K_n 的一个正锥 Q_n, 其中 $A_n\subseteq Q_n$, Q_n 可拓展为 K_{n+1} 的一个正锥 Q_{n+1}, 使得 $A_{n+1}\subseteq Q_{n+1}$. 如此进行下去, 我们得到一个由序域组成的序列:

$(F,P),(K_1,Q_1),\cdots,(K_n,Q_n),\cdots$, 使得 $P\subseteq Q_1\subseteq\cdots\subseteq Q_n\subseteq\cdots$. 令 $Q=\bigcup_{n=1}^{\infty}Q_n$, 则显然 Q 是正锥 P 在 K 上的一个拓展. 这表明, 限制映射 r 是 $\mathcal{X}_K$ 到 C 的一个满射.

设 $Q_1,Q_2\in\mathcal{X}_K$, 且 $Q_1\cap F=Q_2\cap F$, 则 $Q_1\cap K_0=Q_2\cap K_0$. 假定 $Q_1\cap K_n=Q_2\cap K_n$. 令 $Q'=Q_1\cap K_n$, 则 $Q_1\cap K_{n+1}$ 和 $Q_2\cap K_{n+1}$ 都是 Q' 在域 $K_n(A_{n+1})$ 上的拓展, 且 $A_{n+1}\subseteq Q_i\cap K_{n+1}$, $i=1,2$. 注意到, $A_n\subseteq Q'$. 由引理 6.4.2(2) 中的惟一性知, $Q_1\cap K_{n+1}=Q_2\cap K_{n+1}$. 由归纳法原理知, 对于每个非负整数 n, $Q_1\cap K_n=Q_2\cap K_n$. 由此有 $Q_1=Q_1\cap\left(\bigcup_{n=0}^{\infty}K_n\right)=\bigcup_{n=0}^{\infty}(Q_1\cap K_n)=\bigcup_{n=0}^{\infty}(Q_2\cap K_n)=Q_2$. 这表明, 限制映射 r 是一个单射.

注意到, 对于每个 $b\in\dot{F}$, $r^{-1}(H(b)\cap C)=H_K(b)$, 这里 $H_K(b)=\{Q\in\mathcal{X}_K\mid b\in Q\}$. 因而 r 是一个连续映射. 由于 $\mathcal{X}_K$ 是一个紧空间, 且 C 是 $\mathcal{X}_F$ 的一个紧子集, 从而 r 是 $\mathcal{X}_K$ 到 C 的一个同胚映射. 证毕.

引理 6.4.4 设 R 是一个实闭域, x 是 R 上一个未定元, 则存在 $R(x)$ 的一个代数扩张 F, 使得 $\mathcal{X}_F$ 同胚于乘积拓扑空间 $\{1,-1\}^R$, 这里 $\{1,-1\}$ 被赋予离散拓扑.

证明 根据定理 2.6.3, 单超越扩张域 $R(x)$ 有一个正锥 $Q_{+\infty}$, 这个正锥 $Q_{+\infty}$ 是由 R 的分割 $D_{+\infty}=R$ 惟一确定的. 从而对于每个 $a\in R$, $x-a\in Q_{+\infty}$. 对于 $a\in R$, 用 $\sqrt{x-a}$ 表示多项式 $y^2-(x-a)$ 在序域 $(R(x),Q_{+\infty})$ 的实闭包中惟一的正根. 记 $A=\{x-a\mid a\in R\}$, 且 $B=\{\sqrt{x-a}\mid a\in R\}$, 则 $\sqrt{A}\subseteq R(x)(B)$. 此外, 可断言 B 是 A 在 $R(x)$ 上的一个平方根基. 事实上, 如若不然, 则有有限个相异元素 $\sqrt{x-a_1},\cdots,\sqrt{x-a_m}\in B$, 使得 $[R(x)(\sqrt{x-a_1},\cdots,\sqrt{x-a_m}):R(x)]<2^m$. 选取最小的自然数 m, 使得上面不等式成立. 不妨设 $a_1<_{R^2}<_{R^2}\cdots<_{R^2}a_m$. 由 m 的最小性知 $[R(x)(\sqrt{x-a_1},\cdots,\sqrt{x-a_{m-1}}):R(x)]=2^{m-1}$. 由此可知 $\sqrt{x-a_m}\in R(x)(\sqrt{x-a_1},\cdots,\sqrt{x-a_{m-1}})$. 根据定理 2.6.3, 单超越扩张 $R(x)$ 有一个正锥 $Q_{a_{m-1}+}$, 使得 $Q_{a_{m-1}+}$ 是由 R 的分割 $D_{a_{m-1}+}$ 确定的. 此时可知 $x-a_m\notin Q_{a_{m-1}+}$, 但 $x-a_i\in Q_{a_{m-1}+}$, $i=1,\cdots,m-1$. 令 R_1 为序域 $(R(x),Q_{a_{m-1}+})$ 的实闭包, 则显然 $\sqrt{x-a_i}\in R_1$, $i=1,\cdots,m-1$. 于是 $\sqrt{x-a_m}\in R(x)(\sqrt{x-a_1},\cdots,\sqrt{x-a_{m-1}})\subseteq R_1$, 即有 $x-a_m\in R_1^2$. 然而, $x-a_m\in -Q_{a_{m-1}+}\subseteq -R_1^2$, 矛盾.

令 $F=R(x)(B)$, 则 F 是 $R(x)$ 的一个代数扩张. 对于每个 $P\in\mathcal{X}_F$, 可规定这样一个 $\sigma_P\in\{1,-1\}^R$, 使得对于每个 $a\in R$, $\sigma_P(a)=\mathrm{sgn}_P(\sqrt{x-a})$. 因而, 我们得到 $\mathcal{X}_F$ 到 $\{1,-1\}^R$ 的一个映射 σ: $P\longmapsto\sigma_P$, $P\in\mathcal{X}_F$.

设 $P_1,P_2\in\mathcal{X}_F$, 且 $\sigma_{P_1}=\sigma_{P_2}$, 则对每个 $a\in R$, $\mathrm{sgn}_{P_1}(\sqrt{x-a})=\mathrm{sgn}_{P_2}(\sqrt{x-a})$. 令 $\epsilon_a=\mathrm{sgn}_{P_1}(\sqrt{x-a})$, $a\in R$. 由于 B 是 A 在 $R(x)$ 上的一个平方根基, 从而 $B_1=\{\epsilon_a\sqrt{x-a}\mid a\in R\}$ 显然也是 A 在 $R(x)$ 上的一个平方根基. 注意到 $A\subseteq Q_{+\infty}$,

P_1 和 P_2 都是 $Q_{+\infty}$ 在域 $R(x)(B_1)$ 上的拓展, 且 $B_1 \subseteq P_i$, $i=1,2$. 由引理 6.4.2(2) 中惟一性知, $P_1 = P_2$. 这表明 σ 是一个单射.

再设 $\lambda \in \{1,-1\}^R$. 显然, $B_\lambda = \{\lambda(a)\sqrt{x-a} \mid a \in R\}$ 也是 A 在 $R(x)$ 上的一个平方根基. 注意到 $A \subseteq Q_{+\infty}$. 由引理 6.4.2(2) 知, $Q_{+\infty}$ 可拓展为域 $R(x)(B_\lambda)$ 的一个正锥 P, 使得 $B_\lambda \subseteq P$. 显然, $F = R(x)(B_\lambda)$, 即 $P \in \mathcal{X}_F$. 此时, 对于每个 $a \in R$, $\mathrm{sgn}_P(\sqrt{x-a}) = \lambda(a)\mathrm{sgn}_P(\lambda(a)\sqrt{x-a}) = \lambda(a)$. 从而 $\lambda = \sigma_P$. 这表明 σ 是一个满射.

由乘积拓扑的定义知, 由所有形如 $H_a^k = \{\lambda \in \{1,-1\}^R \mid \lambda(a) = k\}$ 的子集组成 $\{1,-1\}^R$ 的一个子基, 其中 $a \in R$, $k = \pm 1$. 很清楚, $\sigma^{-1}(H_a^k) = H_F(k\sqrt{x-a})$, 这里 $H_F(k\sqrt{x-a}) = \{P \in \mathcal{X}_F \mid k\sqrt{x-a} \in P\}$ 为 $\mathcal{X}_F$ 的一个基本开子集. 因而, 映射 σ 是连续的. 由于 $\mathcal{X}_F$ 和 $\{1,-1\}^R$ 都是紧空间, 从而 σ 是一个同胚映射. 证毕.

现在, 我们能够建立如下的 Craven 定理.

定理 6.4.5 (Craven) 对于任意的 Bool 空间 $\mathcal{X}$, 存在一个域 K, 使得 $\mathcal{X}$ 同胚于 $\mathcal{X}_K$.

证明 由命题 6.4.1(2) 知, $\mathcal{X}$ 同胚于某个乘积拓扑空间 $\{1,-1\}^{\mathcal{B}}$ 的一个闭子集, 其中 $\{1,-1\}$ 被赋予离散拓扑. 设 U 是有理数域 $\mathbb{Q}$ 上一个与 $\mathcal{B}$ 具有相同基数的未定元集, 则 $\mathbb{Q}(U)$ 是一个实域. 令 R 是实域 $\mathbb{Q}(U)$ 的任意一个实闭包. 由引理 6.4.4 知, $R(x)$ 有一个代数扩张 F, 使得 $\mathcal{X}_F$ 同胚于乘积拓扑空间 $\{1,-1\}^R$. 将具有相同基数的两个集合 $\mathcal{B}$ 和 U 等同起来, 则有 $\mathcal{B} \subseteq R$. 对于每个 $\lambda \in \{1,-1\}^{\mathcal{B}}$ 以及任意 $a \in R \setminus \mathcal{B}$, 补充规定 $\lambda(a) = 1$. 从而可认定 $\{1,-1\}^{\mathcal{B}} \subseteq \{1,-1\}^R$. 此时, $\{1,-1\}^{\mathcal{B}}$ 显然为 $\{1,-1\}^R$ 的一个闭子集. 因而, $\mathcal{X}$ 实际上同胚于 $\{1,-1\}^R$ 的一个闭子集 C. 根据定理 6.3.3 知, F 是一个 SAP 域. 再由定理 6.4.3 知, 存在 F 的一个代数扩张 K, 使得 $\mathcal{X}_K$ 同胚于 C, 即 $\mathcal{X}_K$ 同胚于 $\mathcal{X}$. 证毕.

在 Craven 的原始论文 [44] 以及后来的其他相关文献 (例如 [155]), 上面定理 6.4.3 的证明都存在欠缺. 有反例表明: 在这些文献的证明中, 所构造的代数扩张 K 根本不满足定理的要求.

§6.5 Pythagoras 域

在本节中, 主要讨论一类特殊域 ——Pythagoras 域以及域的 Pythagoras 闭包.

定义 6.5.1 一个域 F 称作 Pythagoras 域, 如果 $F^2 + F^2 \subseteq F^2$, 即对于任意 $a, b \in F$, 有 $c \in F$, 使得 $a^2 + b^2 = c^2$.

由上面定义 6.5.1 知, 一个域 F 是 Pythagoras 域, 当且仅当 $S_F = F^2$, 当且仅

当对于每个 $a \in F$, $1+a^2 \in F^2$. 显然，二次闭域是非实的 Pythagoras 域，而欧氏域和实闭域是实 Pythagoras 域. 对于非实的 Pythagoras 域，我们有如下刻画.

定理 6.5.1 设域 F 不是一个实域，则 F 是 Pythagoras 域，当且仅当 F 的特征为 2, 或者 F 是二次闭域.

证明 注意到，当 F 的特征为 2 时，对于任意 $a, b \in F$, $a^2+b^2=(a+b)^2$. 从而充分性显然. 下证必要性. 设 F 是 Pythagoras 域，且 F 的特征不为 2, 则由定理 1.1.3 知，$F=S_F=F^2$. 从而对于每个 $a \in F$, 有 $b \in F$, 使得 $a=b^2$. 这表明 F 是二次闭域. 证毕.

由上面定理可见，更值得探讨的 Pythagoras 域应是实 Pythagoras 域. 作为实 Pythagoras 域的一个刻画，我们建立下面的结论.

定理 6.5.2 一个实域 F 是 Pythagoras 域，当且仅当 $F(\sqrt{-1})$ 是 F 的惟一的非实二次扩张.

证明 设 F 是 Pythagoras 域，且 $F(\sqrt{a})$ 是 F 的任意一个非实的二次扩张，其中 $a \in F$, 则有如下关系式:

$$-1=\sum_{i=1}^{n}(b_i+c_i\sqrt{a})^2=\sum_{i=1}^{n}(b_i^2+ac_i^2)+2\sqrt{a}\sum_{i=1}^{n}b_ic_i,$$

其中 $b_i, c_i \in F$, $i=1,\cdots,n$. 此时必有 $\sum_{i=1}^{n}b_ic_i=0$, 即有 $-1=\sum_{i=1}^{n}(b_i^2+ac_i^2)$. 由于 F 是 Pythagoras 域，从而 $1+\sum_{i=1}^{n}b_i^2=b^2$ 且 $\sum_{i=1}^{n}c_i^2=c^2$, 其中 $b, c \in F$, 且 $b \neq 0$. 此时可知 $c \neq 0$, 且有 $\sqrt{a}=-\frac{b}{c}\sqrt{-1}$. 因而有 $F(\sqrt{a})=F(\sqrt{-1})$.

现设 $F(\sqrt{-1})$ 是 F 的惟一的非实二次扩张. 对于任意 $a \in F$, $F(\sqrt{-1-a^2})$ 显然是 F 的一个非实的二次扩张. 由所设知 $F(\sqrt{-1-a^2})=F(\sqrt{-1})$. 从而有 $\sqrt{-1-a^2}=b+c\sqrt{-1}$, 其中 $b, c \in F$, 即有 $-1-a^2=b^2-c^2+2bc\sqrt{-1}$. 此时必有 $bc=0$. 假若 $c=0$, 则有 $-1-a^2=b^2$, 即 $-1=a^2+b^2$, 矛盾于域 F 的实性. 因而 $c \neq 0$, 必然 $b=0$. 由此有 $1+a^2=c^2$. 这表明 F 是一个 Pythagoras 域. 证毕.

借助于 Galois 理论，我们可以进一步建立下面结论.

命题 6.5.3 若域 F 不是 Pythagoras 域，则 F 有一个 4 次循环扩张.

证明 设 F 不是 Pythagoras 域，则对于某个 $a \in F$, $1+a^2 \notin F^2$. 令 $b=1+a^2$, 则 $\sqrt{b} \notin F$. 考虑多项式 $f(x)=(x^2-b)^2-b$. 任意取定域 F 的一个代数闭包 Ω, 则易知 $f(x)$ 在 Ω 中的全部根为 $\alpha=\sqrt{b+\sqrt{b}}$, $\beta=a\alpha^{-1}(\alpha^2-b)$, $-\alpha$ 和 $-\beta$. 于是 $f(x)=(x-\alpha)(x+\alpha)(x-\beta)(x+\beta)$. 假若 $f(x)$ 在 F 上可约，则在 $F[x]$ 中 $f(x)$ 必有这样一个二次因式 $(x-\alpha)(x-\gamma)$, 这里 $\gamma=-\alpha$, β 或 $-\beta$. 由于 $\alpha^2=b+\sqrt{b} \notin F$, 从而 γ

只能为 $\pm\beta$. 于是 $\alpha\beta \in F$, 即对于某个 $c \in F$, $(\alpha\beta)^2 = c^2$. 此时, $a^2(\alpha^2-b)^2 = c^2$, 即 $b = (ca^{-1})^2 \in F^2$, 矛盾. 因而, $f(x)$ 在 F 上不可约的. 令 $K = F(\alpha)$, 则 $[K:F] = 4$. 注意到, $\beta = a\alpha^{-1}(\alpha^2-b) \in K$. 这表明: K 是 $f(x)$ 在 F 上的分裂域. 因此, K 是 F 的一个 Galois 扩张.

由于 β 是 α 的 F- 共轭元, 从而有 $\tau \in \mathrm{Aut}(K/F)$, 使得 $\tau(\alpha) = \beta$. 此时有

$$\tau^2(\alpha) = \tau(\beta) = \tau\big(a\alpha^{-1}(\alpha^2-b)\big) = a\beta^{-1}(\beta^2-b) = \frac{b\alpha(a^2-\alpha^2)}{b(\alpha^2-a^2)} = -\alpha.$$

从而 τ 的阶大于 2, 即 $\mathrm{Aut}(K/F)$ 必为 4 阶循环群. 因而, F 有一个 4 次循环扩张 K. 证毕.

实际上, 当 F 是实域时, 命题 6.5.3 的逆也是成立的.

定理 6.5.4 一个实域 F 为 Pythagoras 域, 当且仅当 F 没有 4 次循环扩张.

证明 充分性由命题 6.5.3 即得, 下证必要性. 设 F 有一个 4 次循环扩张 K, 且 τ 为 Galois 群 $\mathrm{Aut}(K/F)$ 的生成元. 令 H 为由 τ^2 生成的 2 阶循环子群, 且 E 为 H 的稳定子域. 由 Galois 基本定理知 $[K:E] = [E:F] = 2$, 且 $\mathrm{Aut}(K/E) = H$. 由于 F 的特征不为 2, 从而有 $a, b, c \in F$, 使得 $E = F(\sqrt{a})$, 而 $K = E(\sqrt{b+c\sqrt{a}})$.

令 $\alpha = \sqrt{b+c\sqrt{a}}$, 则 $\tau^2(\alpha) = -\alpha$. 由于 $\tau \notin H$, 从而有 $\tau(\sqrt{a}) = -\sqrt{a}$. 此时有 $\tau(\alpha)^2 = \tau(\alpha^2) = \tau(b+c\sqrt{a}) = b - c\sqrt{a}$, 即有 $\big(\alpha\tau(\alpha)\big)^2 = \alpha^2\tau(\alpha)^2 = b^2 - c^2a \in F$.

另一方面, $\tau^2\big(\alpha\tau(\alpha)\big) = \tau^2(\alpha)\tau^3(\alpha) = (-\alpha)\tau(-\alpha) = \alpha\tau(\alpha)$. 从而 $\alpha\tau(\alpha) \in E$, 即有 $x, y \in F$, 使得 $\alpha\tau(\alpha) = x + y\sqrt{a}$. 于是 $b^2 - c^2a = \big(\alpha\tau(\alpha)\big)^2 = (x^2+ay^2) + 2xy\sqrt{a}$. 由此有 $xy = 0$, 即 $x = 0$ 或 $y = 0$. 假若 $y = 0$, 则 $\alpha\tau(\alpha) = x \in F$. 此时, $\tau(\alpha)\tau^2(\alpha) = \tau\big(\alpha\tau(\alpha)\big) = \alpha\tau(\alpha)$, 即有 $\tau^2(\alpha) = \alpha$. 从而 $\alpha = -\alpha$, 矛盾. 因而 $y \neq 0$, 必定 $x = 0$. 由前面等式知, $b^2 - c^2a = ay^2$, 即 $a(c^2+y^2) = b^2$. 如若 $b = 0$, 则由域 F 的实性有 $c = y = 0$, 矛盾. 因而 $b \neq 0$. 注意到, $a \notin F^2$. 从而 $ab^2 \notin F^2$, 即 $(ac)^2 + (ay)^2 \notin F^2$. 这表明 F 不是 Pythagoras 域. 证毕.

根据上面的定理 6.5.4, 容易给出欧氏域的如下一个刻画.

推论 一个实域 E 为欧氏域, 当且仅当对于 E 的每个 2^k 次 Galois 扩张, 总有 $k \leqslant 1$.

证明 设 E 为欧氏域, 且 K 是 E 的一个 2^k 次 Galois 扩张, 则 $G := \mathrm{Aut}(K/E)$ 是一个 2^k 阶的群. 如若 $k > 1$, 则由群论中熟知事实, G 有一个阶为 2^{k-1} 的正规子群 H. 设 L 是 H 的稳定域, 则 $[L:E] = 2$, 且 H 是 K 在 L 上的 Galois 群. 由定理 6.2.3 知, $L = E(\sqrt{-1})$ 是一个二次闭域. 同样可知, L 有一个二次扩张, 矛盾. 从而 $k \leqslant 1$.

反过来, 设 E 满足推论中所给的条件, 则 E 没有 4 次循环扩张. 由定理 6.5.4 知, E 为 Pythagoras 域, 从而 E^2 是 E 的弱亚正锥. 假若 $E \neq E^2 \cup -E^2$, 则

有 $a\in E$, 使得 $a\notin E^2\cup -E^2$. 此时, $E(\sqrt{a})$ 为 E 的一个实二次扩张. 于是, $E(\sqrt{a},\sqrt{-1})$ 是 E 的 4 次扩张, 与所设矛盾. 从而 $E=E^2\cup -E^2$. 因此, E 是一个欧氏域. 证毕.

借助于 Witt 环, 我们可给出 Pythagoras 域的如下刻画:

定理 6.5.5 设 F 是一个特征不为 2 的域, 则有

(1) F 是非实的 Pythagoras 域, 当且仅当 $W(F)\cong \mathbb{Z}/2\mathbb{Z}$;

(2) F 是实 Pythagoras 域, 当且仅当加法群 $(W(F),\oplus)$ 中每个非零元的阶都是无限的, 即 $W(F)$ 是无挠的.

证明 (1) 设 F 是非实的 Pythagoras 域. 由定理 6.5.1 知, F 是二次闭域. 从而对于每个 $a\in \dot{F}$, $\langle a\rangle \approx_F \langle 1\rangle$. 于是对于任意 a, $b\in\dot{F}$, $\langle a,b\rangle\approx_F\langle 1,-1\rangle$, 即 $[\langle a,b\rangle]=[0]$. 因此, $W(F)=\{[0],[\langle 1\rangle]\}$, 即 $W(F)\cong\mathbb{Z}/2\mathbb{Z}$.

反过来, 若 $W(F)\cong\mathbb{Z}/2\mathbb{Z}$, 则 $W(F)=\{[0],[\langle 1\rangle]\}$. 对于任意 $a\in\dot{F}$, $[\langle a\rangle]\neq[0]$. 从而有 $[\langle a\rangle]=[\langle 1\rangle]$, 即有 $\langle a\rangle\approx_F\langle 1\rangle$. 这表明 $a\in F^2$. 因而, F 是二次闭域. 由定理 6.5.1 知, F 是非实的 Pythagoras 域.

(2) 设 F 是一个实 Pythagoras 域. 由命题 5.9.2 知, $W(F)$ 中每个非零元可表为 $[q]$, 其中 q 是域 F 上一个正维数的反迷向型. 假若对于某个正整数 m, $m\times[q]=[0]$, 则 $m\times q$ 是双曲型, 自然是迷向的. 令 $q=\langle a_1,\cdots,a_n\rangle$, 则 F 中有不全为零的元素 e_{ij}, $i=1,\cdots,n$; $j=1,\cdots,m$, 使得 $\sum\limits_{j=1}^{m}\sum\limits_{i=1}^{n}a_ie_{ij}^2=0$, 即 $\sum\limits_{i=1}^{n}a_i\left(\sum\limits_{j=1}^{m}e_{ij}^2\right)=0$. 由于 F 是 Pythagoras 域, 从而 $\sum\limits_{j=1}^{m}e_{ij}^2\in F^2$, 即有 $b_i\in F$, 使得 $\sum\limits_{j=1}^{m}e_{ij}^2=b_i^2$, $i=1,\cdots,n$. 由于 F 是实域, 从而 $b_1,\cdots,b_n$ 不全为零. 此时, $\sum\limits_{i=1}^{n}a_ib_i^2=0$, 矛盾于型 q 的反迷向性. 因此, $W(F)$ 是无挠的.

现设 $W(F)$ 是无挠的. 对于任意 $a\in F$, 当 $1+a^2=0$ 时, 显然 $1+a^2\in F^2$; 当 $1+a^2\neq 0$ 时, 由命题 5.1.5 知, $2\times\langle 1+a^2\rangle\approx_F 2\times\langle 1\rangle$. 由所设知, $\langle 1+a^2\rangle\approx_F\langle 1\rangle$. 由此可知 $1+a^2\in F^2$. 因而, F 是 Pythagoras 域. 假若 F 不是实域, 则由结论 (1) 知, $W(F)\cong\mathbb{Z}/2\mathbb{Z}$, 与所设矛盾. 因此 F 是一个实 Pythagoras 域. 证毕.

一个实 Pythagoras 可能具有多个序, 因而实 Pythagoras 域不一定是欧氏域. 对此, 考虑下面的例子.

例 设 F_0 是一个实 Pythagoras 域, $F_1=F_0((t))$ 是域 F_0 上含未定元 t 的形式幂级数域. 此时, 我们有如下两个断言.

断言 1 F_1 是一个 Pythagoras 域.

设 α 和 β 是 F_1 中任意两个非零元. 由于 F_0 是实 Pythagoras 域, 从而 $\alpha^2+\beta^2$ 可表为

$$\alpha^2+\beta^2=(c_0t^m)^2(1+c_1t+\cdots+c_nt^n+\cdots),$$

其中 $c_i\in F_0$, $i=0,1,2,\cdots$.

令 $\eta=1+c_1t+\cdots+c_nt^n+\cdots$. 注意到, F_1 实际上是系数在 F_0 中而指数在 $\mathbb{Z}$ 中的形式幂级数, 即 $F_1=F_0((\mathbb{Z}))$. 因此, F_1 有自然赋值 v, 使得 v 是一个 Hensel 赋值, 剩余域 $F_v=F_0$, 且值群 $G_v=\mathbb{Z}$. 记 A_v 为 v 的赋值环, 则 $x^2-\eta\in A_v[x]$. 此时, $x^2-\eta\equiv(x+1)(x-1)\ (\mathrm{mod}\,M_v)$, 这里 M_v 是 v 的赋值理想. 由 Hensel 引理知 $x^2-\eta$ 在 A_v 中有根 γ. 由此有 $\eta=\gamma^2$, 进而 $\alpha^2+\beta^2=(c_0t^m\gamma)^2\in F_1^2$. 这表明 F_1 是一个 Pythagoras 域.

此外, 由于 $|G_v/2G_v|=|\mathbb{Z}/2\mathbb{Z}|=2$, 从而由定理 5.6.7 的推论 1 知, 如下断言成立.

断言 2 F_0 的每个序在 F_1 上恰有两个拓展.

当 F_0 为欧氏域时, 由上面两个断言知, F_1 是一个恰有两个序的 Pythagoras 域. 重复上面过程, 可得到域扩张 $F_0\subseteq F_1\subseteq\cdots\subseteq F_n$, 使得 F_i 是 F_{i-1} 上含单变元的形式幂级数域, $i=1,\cdots,n$. 由上面断言和归纳法可知, F_n 是恰有 2^n 个序的 Pythagoras 域. 此外不难知道, 域 $\bigcup\limits_{n=1}^{\infty}F_n$ 是一个具有无限个序的 Pythagoras 域.

设 F 是任意一个域, Ω 为 F 的代数闭包. 显然 Ω 是一个 Pythagoras 域. 记 F_{py} 为 F 和 Ω 的所有 Pythagoras 中间域的交集. 显然 F_{py} 也是一个 Pythagoras 域, 且 $F\subseteq F_{py}\subseteq\Omega$.

定义 6.5.2 如上所得的 Pythagoras 域 F_{py} 称作域 F 在 Ω 中的 Pythagoras 闭包.

由于域 F 的任意两个代数闭包都是 F- 同构的, 从而易知 F 在任意两个代数闭包中的 Pythagoras 闭包是 F- 同构的. 因此, F 的 Pythagoras 闭包在 F- 同构的意义下是惟一的.

显然, F 是 Pythagoras 域, 当且仅当 $F=F_{py}$. 关于域的 Pythagoras 闭包, 可以建立如下事实.

命题 6.5.6 对于一个域 F, 下列结论成立:

(1) 若 K 是 F 的一个 Pythagoras 扩张, 则 K 包含 F 的一个 Pythagoras 闭包;

(2) F 的一个扩张 K 是 F 的 Pythagoras 闭包, 当且仅当 K 是 Pythagoras 域, 且 K 的每个包含 F 的真子域不再为 Pythagoras 域;

(3) 若 F 是实域, 则 F_{py} 也是实域.

证明 (1) 设 E 是 F 在 K 中的代数闭包. 由于 K 是 Pythagoras 域, 从而易知, E 也是一个 Pythagoras 域. 令 Ω 是 E 的代数闭包, 则 Ω 也是 F 的代数闭包. 记 F_{py} 为 F 在 Ω 中的 Pythagoras 闭包, 则由定义知, $F\subseteq F_{py}\subseteq E\subseteq K$.

(2) 必要性显然，下证充分性. 根据结论 (1) 知，$F\subseteq F_{py}\subseteq K$, 这里 F_{py} 是 F 的一个 Pythagoras 闭包. 由所设知必定 $K=F_{py}$.

(3) 由于 F 是实域，从而 F 至少有一个实闭包 R. 注意到 R 是一个 Pythagoras 域. 由结论 (1) 知，$F_{py}\subseteq R$. 因而 F_{py} 是实域. 证毕.

Pythagoras 闭包可通过如下更直接的方式获得.

设 F 是任意域，Ω 为 F 的代数闭包. 规定 Ω 的如下子集:

$$\sqrt{1+F^2}=\{\sqrt{1+a^2}\in\Omega\mid a\in F\}.$$

由此可得 F 和 Ω 的中间域序列: $F\subseteq F_1\subseteq\cdots\subseteq F_n\subseteq\cdots$, 使得 $F_1=F(\sqrt{1+F^2})$, 而 $F_{n+1}=F_n(\sqrt{1+F_n^2})$, $n=1,2,\cdots$. 此时易知，$\bigcup\limits_{n=1}^{\infty}F_n$ 是 F 在 Ω 中的 Pythagoras 闭包.

实域的 Pythagoras 闭包与欧氏包之间有着重要的联系，这种联系反映在下面的定理中.

定理 6.5.7　设 F 是一个实域，Ω 是 F 的代数闭包，则 F 在 Ω 中的 Pythagoras 闭包恰好等于 F 在 Ω 中所有的欧氏包的交.

证明　设 $\{E_\lambda\mid\lambda\in\Lambda\}$ 是由 F 在 Ω 中的全部欧氏包组成的集合. 显然，对于每个 $\lambda\in\Lambda$, E_λ 是包含 F 的 Pythagoras 域. 由 Pythagoras 闭包的定义知，$F_{py}\subseteq E_\lambda$. 因而，$F_{py}\subseteq\bigcap\limits_{\lambda\in\Lambda}E_\lambda$.

假若 $F_{py}\neq\bigcap\limits_{\lambda\in\Lambda}E_\lambda$, 则有 $\alpha\in\bigcap\limits_{\lambda\in\Lambda}E_\lambda$, 但 $\alpha\notin F_{py}$. 对于 Ω 的任意一个 F_{py}- 自同构 π, 易知 $\{\pi(E_\lambda)\mid\lambda\in\Lambda\}$ 也是由 F 在 Ω 中的全部欧氏包组成. 从而 $\pi(\bigcap\limits_{\lambda\in\Lambda}E_\lambda)=\bigcap\limits_{\lambda\in\Lambda}\pi(E_\lambda)=\bigcap\limits_{\lambda\in\Lambda}E_\lambda$. 这表明 $\bigcap\limits_{\lambda\in\Lambda}E_\lambda$ 是 F_{py} 的一个 Galois 扩张. 从而 F_{py} 有一个有限 Galois 扩张 K, 使得 $\alpha\in K$, 且 $K\subseteq\bigcap\limits_{\lambda\in\Lambda}E_\lambda$. 记 $F_{py}\langle 2\rangle$ 是 F_{py} 在 Ω 中的二次闭包，则 $K\subseteq\bigcap\limits_{\lambda\in\Lambda}E_\lambda\subseteq F_{py}\langle 2\rangle$. 由命题 6.2.2 知，$[K:F_{py}]=2^m$, 其中 m 为自然数. 由有限群理论知，$\mathrm{Aut}(K/F_{py})$ 有一个阶为 2^{m-1} 的子群 H. 令 L 是 H 的稳定域. 由 Galois 基本定理知，L 是 F_{py} 的一个扩张次数为 2 的扩张域，且 $L\subseteq K$. 于是 $L=F_{py}(\beta)$, 其中 $\beta^2\in F_{py}$. 设 P 是 F_{py} 的任意一个正锥，且 R 为序域 (F_{py},P) 在 Ω 中的实闭包. 由命题 6.2.4(1) 的证明知，R 包含 F_{py} 的一个欧氏包 E. 显然，E 实际上也是 F 在 Ω 中的一个欧氏包. 从而，$\beta\in E\subseteq R$, 于是 $\beta^2\in R^2\cap F_{py}=P$. 根据定理 1.1.4 知，$\beta^2\in S_{F_{py}}=F_{py}^2$. 由此有 $\beta\in F_{py}$, 即有 $L=F_{py}$, 矛盾. 因而，$F_{py}=\bigcap\limits_{\lambda\in\Lambda}E_\lambda$. 证毕.

命题 6.5.8　设域 F 不是一个 Pythagoras 域，则 F 的 Pythagoras 闭包 F_{py} 包含 F 的一个 4 次循环扩张.

证明 由所设知，有 $a \in F$，使得 $1+a^2 \notin F^2$. 此时，显然 F 的特征不为 2. 令 $b = 1+a^2$，则 $\sqrt{b} \in F_{py}$. 此时有 $b+\sqrt{b} = 1+a^2+\sqrt{1+a^2} = \frac{1}{4}a^2+\frac{1}{4}a^2+\frac{1}{4}(1+\sqrt{b})^2+\frac{1}{4}(1+\sqrt{b})^2 \in S_{F_{py}} = F_{py}^2$. 从而 $\sqrt{b+\sqrt{b}} \in F_{py}$. 根据命题 6.5.3 的证明可知，$F(\sqrt{b+\sqrt{b}})$ 是 F 的一个 4 次循环扩张. 证毕.

推论 设 K 是域 F 的一个有限扩张. 若 K 是 Pythagoras 域，则 F 也是一个 Pythagoras 域.

证明 由命题 6.5.6(1) 知，K 包含 F 的一个 Pythagoras 闭包 F_{py}. 此时，F_{py} 是 F 的一个有限扩张. 假若 $F_{py} \neq F$，则 F_{py} 包含一个真子域 E，使得 $F \subseteq E$，且 F_{py} 和 E 之间没有非浅显的中间域. 由于 $E \neq F_{py}$，从而 E 不可能为 Pythagoras 域. 由上面的命题知，F_{py} 包含 E 的一个 4 次循环扩张 L. 由 Galois 基本定理知，L 和 E 之间有一个中间域 L_1，使得 $[L:L_1]=2$. 于是，L_1 是 F_{py} 和 E 之间一个非浅显的中间域，矛盾. 因而，$F = F_{py}$，即 F 是一个 Pythagoras 域. 证毕.

由上面推论，可知这样一个事实：若域 F 不是一个 Pythagoras 域，则 F 的 Pythagoras 闭包必为 F 的无限代数扩张.

§6.6 遗传 Pythagoras 域

在本节中，我们将引进和讨论一类具有更强性质的 Pythagoras 域 —— 遗传 Pythagoras 域.

定义 6.6.1 一个实域 F 称作遗传 Pythagoras 域，如果 F 及其所有的实代数扩张都是 Pythagoras 域.

显然，所有的实闭域都是遗传 Pythagoras 域. 而且，遗传欧氏域必为遗传 Pythagoras 域.

为讨论的需要以及结论的一般化，我们给出一个更一般的概念 —— 相对遗传 Pythagoras 域.

定义 6.6.2 设 L 是实域 F 的一个代数扩张. 称 F 是一个相对 L 的遗传 Pythagoras 域，如果 F 和 L 的每个实的中间域都是 Pythagoras 域.

由定义可知，定义 6.6.1 中所指的遗传 Pythagoras 域即为相对代数闭包的遗传 Pythagoras 域，它具备这样的绝对意义：相对于每个代数扩张，它都是遗传 Pythagoras 域.

为简便起见，在本节中，始终设 F 是一个实域. 本节的目的是研究相对代数闭包的遗传 Pythagoras 域和相对二次闭包的遗传 Pythagoras 域. 为统一讨论起见，本节用同一符号 Ω 既表示 F 的二次闭包又表示 F 的代数闭包，除非特别指明. 显然，对于 F 和 Ω 的一个中间域 K，K 在 Ω 中是实闭的 (即 K 在 Ω 中没有实的

真扩张), 当且仅当 K 是 F 在 Ω 中的一个欧氏包或实闭包, 根据 Ω 是 F 的二次闭包或代数闭包而定. 此时, 我们称 K 是 Ω- 实闭的, 或称 K 是 F 的一个 Ω- 实闭包 . 不失一般性, 当 Ω 表示 F 的二次闭包时, F 的每个二次扩张都认定在 Ω 中; 而当 Ω 表示 F 的代数闭包时, F 的每个代数扩张也认定在 Ω 中.

在建立主要结论之前, 我们需要建立一些引理.

引理 6.6.1 (1) 若 G 是 Galois 群 $\mathrm{Aut}(\Omega/F)$ 的一个 Abel 子群, 且 K 是 G 的稳定域, 则 Galois 群 $\mathrm{Aut}(\Omega/K)$ 是 $\mathrm{Aut}(\Omega/F)$ 的一个包含 G 的 Abel 子群.

(2) 若 σ 是群 $\mathrm{Aut}(\Omega/F)$ 中一个 2 阶元素, 且 E 是 2 阶循环子群 $\langle\sigma\rangle$ 的稳定域, 则 E 是 Ω- 实闭的. 特别地, $\sigma(\sqrt{-1}) \neq \sqrt{-1}$, 即 $\sigma(\sqrt{-1}) = -\sqrt{-1}$.

证明 (1) 由域论中事实, K 是 F 的 Galois 扩张, 且 $G \subseteq \mathrm{Aut}(\Omega/K)$. 假若 $\mathrm{Aut}(\Omega/K)$ 不是 Abel 子群, 则有 $\tau, \pi \in \mathrm{Aut}(\Omega/K)$, 使得 $\tau\pi \neq \pi\tau$, 即有 $\alpha \in \Omega$, 使得 $\tau\pi(\alpha) \neq \pi\tau(\alpha)$. 设 N 是 $F(\alpha)$ 在 F 上的正规闭包, 且令 $G_N = \{\sigma|_N \mid \sigma \in G\}$, 其中 $\sigma|_N$ 表示 σ 在 N 上的限制, 则 G_N 是 $\mathrm{Aut}(N/F)$ 的一个子群. 容易验证 $K \cap N$ 恰为 G_N 的稳定域. 由有限 Galois 理论知, $\mathrm{Aut}(N/K\cap N) = G_N$. 显然, $\tau|_N$, $\pi|_N \in \mathrm{Aut}(N/K\cap N) = G_N$. 由于 G_N 显然是 Abel 群, 从而 $\tau|_N\pi|_N = \pi|_N\tau|_N$. 由此导致矛盾: $\tau\pi(\alpha) = \tau|_N\pi|_N(\alpha) = \pi|_N\tau|_N(\alpha) = \pi\tau(\alpha)$. 因而 $\mathrm{Aut}(\Omega/K)$ 是一个 Abel 子群.

(2) 由域论中熟知事实 (参见文献 [52]§1.7 中命题 2), $[\Omega : E] = 2$. 当 Ω 是 F 的代数闭包时, 由定理 2.2.1 知, E 是 F 在 Ω 中的实闭包. 当 Ω 是 F 的二次闭包时, 由定理 6.2.5 知, E 是 F 在 Ω 中的欧氏包. 证毕.

引理 6.6.2 设 G 是 Galois 群 $\mathrm{Aut}(\Omega/F)$ 的一个 Abel 子群, 且 E 是 G 的稳定域, 则 $|G| = 2$ 即 E 是 Ω- 实闭的, 或者 E 不是实域.

证明 由域论中的熟知事实知, Ω 是 E 的一个 Galois 扩张. 由引理 6.6.1(1) 知, $\mathrm{Aut}(\Omega/E)$ 也是 $\mathrm{Aut}(\Omega/F)$ 的 Abel 子群, 且 $G \subseteq \mathrm{Aut}(\Omega/E)$.

设 E 是一个实域, 则 E 至少有一个 Ω- 实闭包 R. 此时, $\mathrm{Aut}(\Omega/R)$ 显然是 Abel 群 $\mathrm{Aut}(\Omega/E)$ 的一个 (正规) 子群. 这表明: R 是 E 的一个 Galois 扩张. 由于 R 为实闭域或欧氏域, 从而易知, $\mathrm{Aut}(R/E)$ 仅含有恒等自同构. 因而, $R = E$, 即 E 是一个 Ω- 实闭域. 此时必有 $\Omega = R(\sqrt{-1})$, 且 $|G| = 2$. 证毕.

引理 6.6.3 如果 $G := \mathrm{Aut}(\Omega/F(\sqrt{-1}))$ 是一个 Abel 群, 且 σ 是 $\mathrm{Aut}(\Omega/F)$ 中一个 2 阶元素, 则 $\mathrm{Aut}(\Omega/F) = \langle\sigma\rangle \cdot G$, 且对于每个 $\tau \in G$, $\sigma\tau\sigma = \tau^{-1}$.

证明 由引理 6.6.1(2) 知, $\sigma(\sqrt{-1}) = -\sqrt{-1}$. 从而 $\sigma \notin G$. 注意到 $F(\sqrt{-1})$ 是 F 的一个 Galois 扩张, 从而 G 是 $\mathrm{Aut}(\Omega/F)$ 的正规子群. 由无限 Galois 理论知, $\mathrm{Aut}(\Omega/F)/G \cong \mathrm{Aut}(F(\sqrt{-1})/F)$, 即有 $[\mathrm{Aut}(\Omega/F) : G] = 2$. 此时有 $\mathrm{Aut}(\Omega/F) = \langle\sigma\rangle \cdot G$.

作 $\mathrm{Aut}(\Omega/F)$ 的如下子集:

$$H = \{\sigma\tau\sigma\tau \mid \tau \in G\}.$$

容易验证, $H \subseteq G$. 对于 $\tau, \pi \in G$, 由 G 的交换性有,

$$(\sigma\tau\sigma\tau)(\sigma\pi\sigma\pi) = (\sigma\tau\sigma)\tau(\sigma\pi\sigma)\pi = (\sigma\tau\sigma)(\sigma\pi\sigma)\tau\pi = \sigma(\tau\pi)\sigma(\tau\pi) \in H.$$

因而, H 对于 G 中乘法是封闭的. 此时可进一步知, H 是 G 的一个子群. 设 E 是 H 的稳定域, 则显然 $F(\sqrt{-1}) \subseteq E$. 对于任意 $\tau \in G$, 有 $\tau\sigma\tau\sigma = \tau(\sigma\tau\sigma) = (\sigma\tau\sigma)\tau = \sigma\tau\sigma\tau$. 从而有 $\sigma\tau\sigma\tau\big(\sigma(E)\big) = \sigma(\tau\sigma\tau\sigma)(E) = \sigma(\sigma\tau\sigma\tau)(E) = \sigma(E)$. 于是, $\sigma(E) \subseteq E$. 进一步有 $E = \sigma\big(\sigma(E)\big) \subseteq \sigma(E)$. 因而 $\sigma(E) = E$, 即 $\sigma|_E$ 是域 E 的一个自同构.

设 K 是循环群 $\langle\sigma|_E\rangle$ 的稳定域, 则 $\mathrm{Aut}(E/K) = \langle\sigma|_E\rangle$. 根据无限 Galois 理论知, $\mathrm{Aut}(\Omega/E)$ 是 $\mathrm{Aut}(\Omega/K)$ 的一个正规子群, 且有

$$\mathrm{Aut}(\Omega/K)/\mathrm{Aut}(\Omega/E) \cong \mathrm{Aut}(E/K) = \langle\sigma|_E\rangle.$$

从而 $[\mathrm{Aut}(\Omega/K) : \mathrm{Aut}(\Omega/E)] \leqslant 2$. 注意到, $\sigma \in \mathrm{Aut}(\Omega/K)$, 但 $\sigma \notin \mathrm{Aut}(\Omega/E)$ (否则导致矛盾 $\sigma \in \mathrm{Aut}(\Omega/E) \subseteq G$). 于是 $\mathrm{Aut}(\Omega/K) = \langle\sigma\rangle \cdot \mathrm{Aut}(\Omega/E)$. 显然对于每个 $h \in H$, $\sigma h = h\sigma$, 从而 $\langle\sigma\rangle \cdot H$ 是一个 Abel 子群. 令 L 是 $\langle\sigma\rangle \cdot H$ 的稳定域, 则由 K 的规定知 $L \subseteq K$. 从而 $\mathrm{Aut}(\Omega/K) \subseteq \mathrm{Aut}(\Omega/L)$. 由引理 6.6.1(1) 知, $\mathrm{Aut}(\Omega/L)$ 是一个 Abel 子群, 自然 $\mathrm{Aut}(\Omega/K)$ 也是 $\mathrm{Aut}(\Omega/F)$ 的一个 Abel 子群. 此外, 根据引理 6.6.1(2) 知, K 是一个实域. 再由引理 6.6.2 知, $|\mathrm{Aut}(\Omega/K)| = 2$. 注意到 $H \subseteq \mathrm{Aut}(\Omega/E) \subseteq \mathrm{Aut}(\Omega/K)$, 从而有 $|\langle\sigma\rangle \cdot H| = 2$. 此时必有 $|H| = 1$. 证毕.

引理 6.6.4 设 $F\langle 2\rangle$ 是实域 F 的二次闭包, 则下列叙述等价:

(1) F 是一个相对 $F\langle 2\rangle$ 的遗传 Pythagoras 域;

(2) 对于 F 和 $F\langle 2\rangle$ 的每个非实的中间域 L, $\sqrt{-1} \in L$;

(3) Galois 群 $\mathrm{Aut}(F\langle 2\rangle/F(\sqrt{-1}))$ 是 Abel 群.

证明 (1) $\Longrightarrow$ (2): 由于 -1 在 L 中的平方和表示仅涉及 L 中有限个元素, 从而可假定 L 是 F 的有限扩张. 由二次闭包 $F\langle 2\rangle$ 的构造知, 有这样的一系列域: $F := L_0 \subset L_1 \subset \cdots \subset L_s \subset F\langle 2\rangle$, 使得 $L \subseteq L_s$, 且 $[L_i : L_{i-1}] = 2$, $i = 1, \cdots, s$. 选取最大的下标 m, 使得 $L_m \cap L$ 为实域, 则 $m < s$, 且 $L_{m+1} \cap L$ 不再是实域. 由叙述 (1) 知, $L_m \cap L$ 为 Pythagoras 域. 根据定理 6.5.2 知, $\sqrt{-1} \in L_{m+1} \cap L \subseteq L$.

(2) $\Longrightarrow$ (3): 记 $G = \mathrm{Aut}\big(F\langle 2\rangle/F(\sqrt{-1})\big)$, 且令 E 是 F 在 $F\langle 2\rangle$ 中的一个欧氏包, 则 $\mathrm{Aut}(F\langle 2\rangle/E)$ 是一个 2 阶循环群. 令 σ 是 $\mathrm{Aut}(F\langle 2\rangle/E)$ 的生成元. 此时有 $\mathrm{Aut}(F\langle 2\rangle/F) = \langle\sigma\rangle \cdot G$. 对于任意给定的 $\tau \in G$, 令 L 是循环群 $\langle\sigma\tau\rangle$ 的稳定域. 由于 $\sigma\tau(\sqrt{-1}) = -\sqrt{-1}$, 从而 $\sqrt{-1} \notin L$. 由叙述 (2) 知, L 是一个实域. 根据引理

6.6.2 知，$(\sigma\tau)^2$ 为恒等自同构. 这表明：对于每个 $\tau \in G$, $\sigma\tau\sigma = \tau^{-1}$. 此时易见，$G$ 是一个 Abel 群.

(3) $\Longrightarrow$ (1): 设 K 是 F 和 $F\langle 2\rangle$ 的任意一个实的中间域，且 L 是 K 的一个非实的二次扩张. 用 G 表示 Galois 群 $\mathrm{Aut}(F\langle 2\rangle/K(\sqrt{-1}))$. 由于 G 是 Abel 群 $\mathrm{Aut}(F\langle 2\rangle/F(\sqrt{-1}))$ 的一个子群，从而 G 是 $\mathrm{Aut}(F\langle 2\rangle/K)$ 的一个 Abel 子群. 设 E 是 K 在 $F\langle 2\rangle$ 中的一个欧氏包，则 $\mathrm{Aut}(F\langle 2\rangle/E)$ 是一个具有生成元 σ 的 2 阶循环子群. 根据引理 6.6.1(2) 和 6.6.3 知，$\mathrm{Aut}(F\langle 2\rangle/L) \subseteq \mathrm{Aut}(F\langle 2\rangle/K(\sqrt{-1}))$. 从而有 $\sqrt{-1} \in L$, 即有 $L = K(\sqrt{-1})$. 由定理 6.5.2 知，K 是一个 Pythagoras 域. 证毕.

为了刻画相对二次闭包的遗传 Pythagoras 域，我们还需要如下定义.

定义 6.6.3 域 F 的一个亚正锥 T 称作扇锥，如果对于乘法群 $\dot{F}$ 的任意一个指标为 2 的子群 U, $U \cup \{0\}$ 是 F 的一个正锥，只要 $\dot{T} \subseteq U$, 且 $-1 \notin U$.

容易证明这样一个有用事实：域 F 的一个亚正锥 T 是扇锥，当且仅当对于每个 $b \in F\setminus -T$, $T + bT = T \cup bT$. 事实上，总有 $T \cup bT \subseteq T + bT$. 如若 $T + bT \neq T \cup bT$, 则对于某两个非零元 $t_1, t_2 \in T$, $t_1 + bt_2 \notin T \cup bT$. 注意到，$H := \dot{T} \cup b\dot{T}$ 是 $\dot{F}$ 的一个子群，且商群 $\dot{F}/H$ 中每个非单位元的元素的阶都是 2. 从而 $\dot{F}/H$ 可看作域 $\mathbb{Z}/(2)$ 上一个向量空间. 由所设可知，$-H$, $-(t_1 + bt_2)H$ 作为向量空间 $\dot{F}/H$ 中元素是线性无关的. 从而，线性无关组 $\{-H, -(t_1 + bt_2)H\}$ 可扩充为向量空间 $\dot{F}/H$ 的一个基 $\mathcal{B}$. 令 $\overline{U}$ 是由 $\mathcal{B}\setminus\{-H\}$ 生成的子空间，且 U 是 $\overline{U}$ 在自然同态：$\dot{F} \longrightarrow \dot{F}/H$ 下的原像，则显然 $[\dot{F} : U] = 2$, $\dot{T} \subseteq U$, 且 $-1 \notin U$. 此时易知，$U \cup \{0\}$ 不是 F 的一个正锥. 因而，T 不是一个扇锥. 反过来，若 T 不是一个扇锥，则 $\dot{F}$ 有一个指标为 2 的子群 U, 使得 $\dot{T} \subseteq U$, 且 $-1 \notin U$, 但 $U \cup \{0\}$ 不是 F 的一个正锥. 由正锥的定义知，U 对于加法不是封闭的，即有 $\alpha, \beta \in U$, 使得 $\alpha + \beta \notin U$. 令 $b = \alpha^{-1}\beta$, 则有 $b \in U$, 但 $1 + b \notin U$. 显然，$b \notin -T$; 否则 $-1 = b^{-1}(-b) \in U$! 此时易见，$1 + b \in T + bT$, 但 $1 + b \notin T \cup bT$. 因而 $T + bT \neq T \cup bT$.

现在，我们建立下面命题，这一命题刻画了相对二次闭包的遗传 Pythagoras 域.

命题 6.6.5 一个实域 F 是相对其二次闭包 $F\langle 2\rangle$ 的遗传 Pythagoras 域，当且仅当 F^2 是一个扇锥.

证明 设 F 是相对 $F\langle 2\rangle$ 的一个遗传 Pythagoras 域，则 F 自身显然是 Pythagoras 域. 于是，F^2 是 F 的弱亚正锥. 对于 $a \in F\setminus -F^2$, 显然 $F(\sqrt{a})$ 是 $F\langle 2\rangle$ 的一个实子域. 由所设知，$F(\sqrt{a})$ 是 Pythagoras 域. 从而对于任意 $b, c \in F$, $b^2 + ac^2 \in F(\sqrt{a})^2$. 于是有 $d, e \in F$, 使得 $b^2 + ac^2 = (d + e\sqrt{a})^2 = (d^2 + ae^2) + 2de\sqrt{a}$. 由此有 $de = 0$, 即有 $b^2 + ac^2 = d^2$ 或 ae^2. 这表明 $F^2 + aF^2 \subseteq F^2 \cup aF^2$, 即 $F^2 + aF^2 = F^2 \cup aF^2$. 因而 F^2 是一个扇锥.

反过来，设 F^2 是域 F 的一个扇锥，且 K 是 F 和 $F\langle 2\rangle$ 的任意一个实的中间

域. 不失一般性, 可进一步假定 K 是 F 的有限扩张. 令 E 是 K 在二次闭包 $F\langle 2\rangle$ 中的一个欧氏包, 则存在这样的一系列扩张 $F := L_0 \subset L_1 \subset \cdots \subset L_m \subseteq E$, 使得 $K \subseteq L_m$, 且 $L_i = L_{i-1}(\sqrt{a_{i-1}})$, 其中 $a_{i-1} \in L_{i-1}$, $i = 1, \cdots, m$.

对于 $\alpha \in L_1$, 用 $N(\alpha)$ 表示 α 在 F 上的范数. 作 $\dot{L}_1$ 到 $N(\dot{L}_1)/\dot{F}^2$ 的如下一个映射:

$$\phi:\quad \alpha \longmapsto N(\alpha)\dot{F}^2, \quad \forall \alpha \in \dot{L}_1.$$

显然, ϕ 是乘法群 $\dot{L}_1$ 到 $N(\dot{L}_1)/\dot{F}^2$ 的一个满同态, 使得 $\dot{F}\dot{L}_1^2 \subseteq \ker(\phi)$. 设 $b+c\sqrt{a_0} \in \ker(\phi)$, 其中 $b, c \in F$, 则 $b^2 - a_0c^2 = d^2$, 其中 $d \in \dot{F}$. 由线性方程组的理论, F 上如下线性方程组:

$$\begin{cases} (b-d)x + ca_0y &= 0 \\ cx + (b+d)y &= 0 \end{cases}$$

在 F 中有非零解 (u,v). 于是 $b + c\sqrt{a_0} = d\dfrac{u - v\sqrt{a_0}}{u + v\sqrt{a_0}} = \dfrac{d}{u^2 - a_0v^2}(u - v\sqrt{a_0})^2 \in \dot{F}\dot{L}_1^2$. 由群同态基本定理知, $\dot{L}_1/\dot{F}\dot{L}_1^2 \cong N(\dot{L}_1)\dot{F}^2$. 注意到 $N(\dot{L}_1) = \dot{F}^2 - a_0\dot{F}^2 = \dot{F}^2 \cup -a_0\dot{F}^2$, 从而 $N(\dot{L}_1)/\dot{F}^2 = \{\dot{F}^2, -a_0\dot{F}^2\}$. 从而 $[\dot{L}_1 : \dot{F}\dot{L}_1^2] = 2$, 即有 $\dot{L}_1 = \dot{F}\dot{L}_1^2 \cup \sqrt{a_0}\dot{F}\dot{L}_1^2$. 现设 U 是 $\dot{L}_1$ 的任意一个指标为 2 的子群, 使得 $\dot{L}_1^2 \subseteq U$ 且 $-1 \notin U$. 令 $P = (U \cap F) \cup \{0\}$. 注意到 $\dot{L}_1/U = \dot{F}U/U \cong \dot{F}/\dot{P}$, 从而 $\dot{P}$ 是 $\dot{F}$ 的一个指标为 2 的子群. 显然, $\dot{F}^2 \subseteq \dot{P}$ 且 $-1 \notin \dot{P}$. 由于 F^2 是扇锥, 从而 P 是 F 的一个正锥. 由于 $a_0 \in \dot{P}$, 从而由定理 2.3.8 的推论 2 知, 正锥 P 在 L_1 恰好有两个拓展 Q_1 和 Q_2. 由于 $\dot{L}_1 = \dot{F}\dot{L}_1^2 \cup \sqrt{a}_0\dot{F}\dot{L}_1^2$, 从而 $[\dot{L}_1 : \dot{P}\dot{L}_1^2] = 4$. 注意到 $[\dot{L}_1 : \dot{Q}_1] = 2$, $[\dot{Q}_1 : (\dot{Q}_1 \cap \dot{Q}_2)] = [\dot{Q}_1\dot{Q}_2 : \dot{Q}_2] = [\dot{F} : \dot{Q}_2] = 2$, 且 $\dot{P}\dot{L}_1^2 \subseteq \dot{Q}_1 \cap \dot{Q}_2$. 因而 $\dot{P}\dot{L}_1^2 = \dot{Q}_1 \cap \dot{Q}_2$. 设 $b \in L_1$, 但 $-b \notin Q_1 \cap Q_2$. 当 $b \in Q_1 \cap Q_2$ 时, 显然 $Q_1 \cap Q_2 + b(Q_1 \cap Q_2) = Q_1 \cap Q_2$. 当 $b \notin Q_1 \cap Q_2$ 时, 易知 $\dot{L} = (\dot{Q}_1 \cap \dot{Q}_2) \cup -(\dot{Q}_1 \cap \dot{Q}_2) \cup b(\dot{Q}_1 \cap \dot{Q}_2) \cup -b(\dot{Q}_1 \cap \dot{Q}_2)$. 此时可知, 对于任意 $t_1, t_2 \in \dot{Q}_1 \cap \dot{Q}_2$, $t_1 + bt_2 \notin -(\dot{Q}_1 \cap \dot{Q}_2) \cup -b(\dot{Q}_1 \cap \dot{Q}_2)$. 从而必有 $t_1 + bt_2 \in (\dot{Q}_1 \cap \dot{Q}_2) \cup b(\dot{Q}_1 \cap \dot{Q}_2)$. 这表明: $Q_1 \cap Q_2$ 是 L_1 的一个扇锥. 由于 $\dot{Q}_1 \cap \dot{Q}_2 = \dot{P}\dot{L}_1^2 \subseteq U$, 从而 $U \cup \{0\}$ 是 L_1 的一个正锥. 由 U 的所设条件知, L_1^2 是 L_1 的一个扇锥.

借助于归纳法可得, L_m^2 是 L_m 的一个扇锥. 此时, L_m 当然是 Pythagoras 域. 根据命题 6.5.8 的推论知, K 是一个 Pythagoras 域. 因此, F 是相对 $F\langle 2\rangle$ 的遗传 Pythagoras 域. 证毕.

引理 6.6.6 设 L 是 F 的一个有限扩张, 且 L 相对它的二次闭包是遗传 Pythagoras 域, 则有非负整数 t, 使得下列条件成立:

(1) $[\dot{L} : \dot{F}\dot{L}^2] = 2^t$;

(2) F 的每个在 L 上可拓展的序在 L 上恰有 2^t 个拓展.

证明 设 P 是 F 的一个在 L 上可拓展的正锥. 由命题 6.6.5 知, L^2 是 L 的一个扇锥. 此时, PL^2 必是 L 的一个扇锥. 由此易见, P 在 L 上的拓展与商群 $\dot{L}/P\dot{L}^2$ 的指标为 2 且不包含 $-P\dot{L}^2$ 的子群是一一对应的. 由定理 2.3.8 知, P 在 L 上只有有限个拓展. 从而 $\dot{L}/P\dot{L}^2$ 的指标为 2 且不包含 $-P\dot{L}^2$ 的子群只有有限个. 注意到, $\dot{L}/P\dot{L}^2$ 可看作域 $\mathbb{Z}/(2)$ 上向量空间, 而它的指标为 2 的子群恰为极大子空间. 从而 $\dot{L}/P\dot{L}^2$ 是一个 $\mathbb{Z}/(2)$ 上有限维空间. 令 $t+1$ 为向量空间 $\dot{L}/P\dot{L}^2$ 的维数, 其中 $t \geqslant 0$, 则有 $[\dot{L} : P\dot{L}^2] = 2^{t+1}$. 由于 $[\dot{F}\dot{L}^2 : P\dot{L}^2] = 2$, 从而有 $[\dot{L} : \dot{F}\dot{L}^2] = 2^t$. 此外, 容易证明 $\dot{L}/P\dot{L}^2$ 恰有 2^t 个不包含 $-P\dot{L}^2$ 的极大子空间. 从而引理获证. 证毕.

推论 1 所设同引理 6.6.6, 且设 $[L:F]$ 为奇数, 则 F 的每个在 L 上可拓展的正锥 P 仅有惟一的拓展 PL^2.

证明 由本原元定理, 可设 $L = F(\alpha)$. 令 m 为 P 在 L 上的拓展个数. 由定理 2.1.3 的推论和定理 2.3.8 知, m 与扩张次数 $[L:F]$ 具有相同的奇偶性. 从而 m 是一个奇数. 由引理 6.6.6 知, $m = 2^t$, 其中 $t \geqslant 0$. 此时必有 $t = 0$, 即 P 在 L 上仅有惟一拓展. 注意到 $PL^2 = S_L(P)$, 这里 $S_L(P)$ 的意义如 §1.3 中所示. 由命题 1.3.2 可知, 这个惟一拓展为 PL^2. 证毕.

推论 2 所设同引理 6.6.6, 且设 L 是 F 的一个 Galois 扩张, 则 $[L:K] = 2^t$, 其中 t 是非负整数.

证明 取定 L 的一个正锥 Q, 且令 $P = Q \cap F$. 设 R 是序域 (L, Q) 的实闭包, 则 R 也是 (F, P) 的实闭包. 注意到, L 到 R 中的 F- 嵌入实际上是 L 上的 F- 自同构, 因为 L 是 F 的正规扩张. 根据定理 2.3.8, P 在 L 上的拓展个数等于群 $\mathrm{Aut}(L/F)$ 的阶. 另一方面, 由引理 6.6.6 知, P 在 L 上的拓展个数为 2^t, 其中 $t \geqslant 0$. 因而, $[L:F] = |\mathrm{Aut}(L/F)| = 2^t$. 证毕.

引理 6.6.7 如果 F 是一个欧氏域, 同时又是相对 Ω 的遗传 Pythagoras 域, 那么 F 是相对 Ω 的遗传欧氏域 (即 F 在 Ω 中的每个实扩张都是欧氏域), Galois 群 $\mathrm{Aut}(\Omega/F(\sqrt{-1}))$ 是一个 Abel 群, 且 $F(\sqrt{-1})$ 在 Ω 中的每个有限扩张都是奇次数扩张.

证明 若 Ω 表示 F 的二次闭包, 则 $\Omega = F(\sqrt{-1})$. 此时, 引理显然成立. 现设 Ω 表示 F 的代数闭包, 则 F 是遗传 Pythagoras 域. 考察如下集合:

$$\Xi = \{\ \Delta \mid \Delta\text{是}F\text{和}\Omega\text{的中间域, 使得对于每个}\alpha \in \Delta,\ F(\alpha)\text{是}F\text{的奇次数扩张}\}.$$

由 Zorn 引理, Ξ 中有一个极大中间域 L. 假若 $-1 = \alpha_1^2 + \cdots + \alpha_n^2$, 其中 $\alpha_i \in L$, $i = 1, \cdots, n$. 由本原元定理知 $F(\alpha_1, \cdots, \alpha_n) = F(\alpha)$. 由于 $L \in \Xi$, 从而 $F(\alpha)$ 是 F

的奇次数扩张. 由定理 1.3.4 的推论 1, $F(\alpha)$ 是一个实域, 矛盾. 因而 L 是 F 的一个实代数扩张. 由所设知, L 是一个 Pythagoras 域. 假若 L 有两个相异的正锥 Q_1 和 Q_2, 则有某个 $\alpha \in L$, 使得 $Q_1 \cap F(\alpha) \neq Q_2 \cap F(\alpha)$. 由于 F 是欧氏域, 从而 F 有惟一正锥 F^2. 然而, $F(\alpha)$ 是一个遗传 Pythagoras 域, 当然也是相对它的二次闭包的遗传 Pythagoras 域. 由命题 6.6.5 的推论 1 知, F^2 在 $F(\alpha)$ 上仅有惟一拓展. 这意味着 $Q_1 \cap F(\alpha) = Q_2 \cap F(\alpha)$, 矛盾. 因而, L 仅有惟一正锥, 即 L 是一个欧氏域. 设 N 是 L 在 Ω 中的任意一个有限 Galois 扩张, 令 H 是 $\mathrm{Aut}(N/L)$ 的 Sylow 2- 子群, 且记 E 为 H 的稳定域, 则 E 是 L 的一个奇次数扩张. 易知, $E \in \Xi$. 由 L 的极大性知, $L = E$. 此时, $\mathrm{Aut}(N/L)$ 是一个阶为 2^k 的 Galois 扩张, 其中 2^k 为子群 H 的阶. 由定理 6.5.4 的推论知, $k \leqslant 1$. 这意味着: $\Omega = L(\sqrt{-1})$. 对于 $F(\sqrt{-1})$ 的每个有限扩张 K, 有 $\alpha_1, \cdots, \alpha_r \in L$, 使得 $K = F(\sqrt{-1})(\alpha_1, \cdots, \alpha_n)$. 通过本原元定理可知, $[K : F(\sqrt{-1})]$ 为奇数.

令 $G = \mathrm{Aut}\big(\Omega/F(\sqrt{-1})\big)$, 且取定 $\mathrm{Aut}(\Omega/F)$ 中一个 2 阶元素 σ. 对于 $\tau \in G$, 记 E 是循环子群 $\langle \sigma\tau \rangle$ 的稳定域. 由引理 6.6.2 知, $(\sigma\tau)^2$ 为恒等自同构, 或者 E 不是实域. 假若 E 不是实域, 则 E 有一个非实的子域 E_1, 使得 E_1 是 F 的有限扩张. 显然 $[E_1 : F]$ 为偶数, 此时有

$$2[E_1(\sqrt{-1}) : F(\sqrt{-1})] = [E_1(\sqrt{-1}) : F] = [E_1(\sqrt{-1}) : E_1][E_1 : F].$$

由上面的讨论知, $[E_1(\sqrt{-1}) : F(\sqrt{-1})]$ 为奇数, 从而 $[E_1(\sqrt{-1}) : E_1]$ 为奇数, 即有 $\sqrt{-1} \in E_1$. 然而, 由引理 6.6.1 知, $\sigma\tau(\sqrt{-1}) = \sigma(\sqrt{-1}) = -\sqrt{-1}$, 矛盾. 因而, E 是一个实域. 从而, $(\sigma\tau)^2$ 为恒等自同构, 即 $\sigma\tau\sigma = \tau^{-1}$. 这表明 G 是一个 Abel 群.

再设 F_1 是 F 的任意一个有限实扩张. 由条件知, F_1 是遗传 Pythagoras 域. 对于 F_1 的任意一个正锥 P_1, (F_1, P_1) 是 (F, F^2) 的序代数扩张. 注意到, 上面的域 L 是序域 (F, F^2) 的实闭包. 根据定理 2.3.6 可知, 存在 F_1 到 L 中一个嵌入. 因而, F_1 可看作 L 的一个有限子域. 由本原元定理可知, $[F_1 : F]$ 为奇数. 再由命题 6.6.6 的推论 1 知, F_1^2 是正锥 F^2 在 F_1 上的拓展. 从而 F_1^2 是 F_1 的惟一序. 因而, F_1 是欧氏域. 由于 F 的任意一个实代数扩张是它所包含的全部 F 的有限扩张的并, 从而它是欧氏域的并. 因而, F 的每个实代数扩张都是欧氏域. 证毕.

现在, 我们可建立如下重要结论.

定理 6.6.8 设 F 是一个实域, 则下列叙述等价:

(1) F 是一个相对 Ω 的遗传 Pythagoras 域;

(2) Galois 群 $\mathrm{Aut}\big(\Omega/F(\sqrt{-1})\big)$ 是一个 Abel 群;

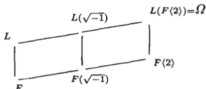
(3) F 在 Ω 中的每个非实的扩张都包含 $\sqrt{-1}$;

(4)F 在 Ω 中的每个实扩张是它的所有 Ω- 实闭包的交.

证明 (1) $\Longrightarrow$ (2): 设 F 是相对 Ω 的遗传 Pythagoras 域, 则 F 是相对二次闭包 $F\langle 2\rangle$ 的遗传 Pythagoras 域. 由引理 6.6.4 知, $\mathrm{Aut}\big(F\langle 2\rangle/F(\sqrt{-1})\big)$ 是 Abel 群. 设 E 是域 F 的任意一个欧氏包, 则 $F\langle 2\rangle = E(\sqrt{-1})$. 由引理 6.6.7 可知, $\mathrm{Aut}(\Omega/F\langle 2\rangle)$ 也是 Abel 群, 且对于 $F\langle 2\rangle$ 在 Ω 中的每个有限扩张 K, $[K : F\langle 2\rangle]$ 为奇数.

设集合 Ξ 如引理 6.6.7 的证明中所示, 且 L 是 Ξ 中的极大中间域. 同样可知, L 是 F 的实代数扩张, Ω 为 L 的二次闭包, 即 $\Omega = L\langle 2\rangle$, 且对于 F 在 L 中每个有限扩张 Δ, $[\Delta(\sqrt{-1}) : F(\sqrt{-1})]$ 为奇数.

设 K 是 $F\langle 2\rangle$ 在 Ω 中任意一个有限的 Galois 扩张, 则 $[K : F\langle 2\rangle]$ 为奇数. 由本原元定理知, $K = F\langle 2\rangle(\alpha)$, 其中 $\alpha \in K$. 此时有 $L(K) = L(F\langle 2\rangle)(\alpha)$, 从而 $L(K)$ 是 $L(F\langle 2\rangle)$ 的有限扩张. 显然, $L(F\langle 2\rangle)$ 的二次闭包仍为 $L\langle 2\rangle$ (即 Ω). 由命题 6.2.2(4) 知, $[L(K) : L(F\langle 2\rangle)]$ 是 2 的方幂. 由域论的一个熟知事实知, $\mathrm{Aut}\big(L(K)/L(F\langle 2\rangle)\big)$ 同构于 $\mathrm{Aut}(K/F\langle 2\rangle)$ 的一个子群. 从而 $[L(K) : L(F\langle 2\rangle)]$ 是 $[K : F\langle 2\rangle]$ 的因数. 此时必有 $[L(K) : L(F\langle 2\rangle)] = 1$, 即有 $K \subseteq L(K) = L(F\langle 2\rangle)$. 由 K 的任意性可知, $\Omega \subseteq L(F\langle 2\rangle)$, 即有 $\Omega = L(F\langle 2\rangle)$. 因此, 我们有如下关于域扩张的示意图:



作群 $\mathrm{Aut}\big(\Omega/L(\sqrt{-1})\big)$ 到 $\mathrm{Aut}\big(F\langle 2\rangle/F(\sqrt{-1})\big)$ 的如下映射:

$$\phi:\quad \tau \longrightarrow \tau|_{F\langle 2\rangle},\quad \forall \tau \in \mathrm{Aut}\big(\Omega/L(\sqrt{-1})\big).$$

易知, ϕ 是一个单同态.

由于 $\mathrm{Aut}\big(F\langle 2\rangle/F(\sqrt{-1})\big)$ 是 Abel 群, 从而 $\mathrm{Aut}\big(\Omega/L(\sqrt{-1})\big)$ 也是一个 Abel 群.

又设 Δ 是 F 在 L 中的任意一个有限扩张, 则 $[\Delta(\sqrt{-1}) : F(\sqrt{-1})]$ 为奇数. 注意到, $F \subseteq F(\sqrt{-1}) \subseteq \Delta(\sqrt{-1}) \cap F\langle 2\rangle \subseteq F\langle 2\rangle$. 由命题 6.2.2(4) 可知, $[\Delta(\sqrt{-1}) \cap F\langle 2\rangle : F(\sqrt{-1})]$ 为 2 的方幂. 又由于 $[\Delta(\sqrt{-1}) \cap F\langle 2\rangle : F(\sqrt{-1})]$ 整除 $[\Delta(\sqrt{-1}) : F(\sqrt{-1})]$, 从而有 $[\Delta(\sqrt{-1}) \cap F\langle 2\rangle : F(\sqrt{-1})] = 1$, 即 $\Delta(\sqrt{-1}) \cap F\langle 2\rangle = F(\sqrt{-1})$. 由 Δ 的任意性知, $L(\sqrt{-1}) \cap F\langle 2\rangle = F(\sqrt{-1})$. 因而, $\mathrm{Aut}\big(\Omega/F(\sqrt{-1})\big)$ 是群 $\mathrm{Aut}(\Omega/F)$ 中由 $\mathrm{Aut}\big(\Omega/L(\sqrt{-1})\big)$ 和 $\mathrm{Aut}(\Omega/F\langle 2\rangle)$ 生成的子群.

为证明 $\mathrm{Aut}\big(\Omega/F(\sqrt{-1})\big)$ 的交换性, 只须证明: $\mathrm{Aut}\big(\Omega/L(\sqrt{-1})\big)$ 中元素和 $\mathrm{Aut}(\Omega/F\langle 2\rangle)$ 中元素可交换.

设 σ 是 $\mathrm{Aut}(\Omega/L)$ 中任意 2 阶元素 (这样的元素必定存在), 且 E 为循环群 $\langle \sigma|_{F\langle 2\rangle}\rangle$ 的稳定域, 则 E 是 F 的一个欧氏包, 且 $F\langle 2\rangle = E(\sqrt{-1})$. 由前面的说明

知, $\operatorname{Aut}(\Omega/E(\sqrt{-1}))$ 是 Abel 群. 由引理 6.6.3 知, 对于任意 $\tau\in\operatorname{Aut}(\Omega/F\langle 2\rangle)$, $\sigma\tau$ 的阶为 2. 对于 $\pi\in\operatorname{Aut}(\Omega/L(\sqrt{-1}))$, 由引理 6.6.3 同样可知, $\sigma\pi$ 的阶为 2. 注意到 $\sigma\pi\in\operatorname{Aut}(\Omega/L)$, 从而又有 $(\sigma\pi)\tau(\sigma\pi)=\tau^{-1}$, 即 $\pi\tau=\sigma\tau^{-1}\pi^{-1}\sigma$. 由此有

$$\pi\tau=\sigma\tau^{-1}\pi^{-1}\sigma=\sigma(\sigma\tau\sigma)(\sigma\pi\sigma)\sigma=\tau\pi.$$

因此, $\operatorname{Aut}(\Omega/F(\sqrt{-1}))$ 是 Abel 群.

(2) $\Longrightarrow$ (3): 设 K 是 F 在 Ω 中的一个非实的扩张. 由引理 6.6.1(2) 知, Galois 群 $\operatorname{Aut}(\Omega/K)$ 中不能包含 2 阶元素. 根据引理 6.6.3 知, 对于 $\operatorname{Aut}(\Omega/F)$ 中一个阶为 2 的元素 σ, 有 $\operatorname{Aut}(\Omega/F)=\langle\sigma\rangle\cdot\operatorname{Aut}(\Omega/F(\sqrt{-1}))$, 且陪集 $\sigma\operatorname{Aut}(\Omega/F(\sqrt{-1}))$ 中元素的阶均为 2. 注意到如下关系:

$$\operatorname{Aut}(\Omega/K)\subseteq\operatorname{Aut}(\Omega/F)=\operatorname{Aut}(\Omega/F(\sqrt{-1}))\cup\sigma\operatorname{Aut}(\Omega/F(\sqrt{-1})).$$

从而 $\operatorname{Aut}(\Omega/K)\subseteq\operatorname{Aut}(\Omega/F(\sqrt{-1}))$, 即有 $\sqrt{-1}\in K$.

(3) $\Longrightarrow$ (1): 设 K 是 F 在 Ω 中的一个实扩张, 且 L 是 K 的一个非实的二次扩张. 由叙述 (3) 知, $\sqrt{-1}\in L$, 即有 $L=K(\sqrt{-1})$. 由定理 6.5.2 知, K 是一个 Pythagoras 域. 由定义知, K 是相对于 Ω 的遗传 Pythagoras 域.

(2) $\Longrightarrow$ (4): 设 K 是 F 在 Ω 中任意一个实扩张, 则 $\operatorname{Aut}(\Omega/K(\sqrt{-1}))$ 是 $\operatorname{Aut}(\Omega/F(\sqrt{-1}))$ 的一个子群. 由叙述 (2) 知, $\operatorname{Aut}(\Omega/K(\sqrt{-1}))$ 也是一个 Abel 群. 由引理 6.6.3 知, $\operatorname{Aut}(\Omega/K)=\langle\sigma\rangle\cdot\operatorname{Aut}(\Omega/K(\sqrt{-1}))$, 其中 σ 是 $\operatorname{Aut}(\Omega/K)$ 中一个 2 阶元素, 且陪集 $\sigma\operatorname{Aut}(\Omega/K(\sqrt{-1}))$ 中元素的阶均为 2.

为证明叙述 (4), 仅须证明这样一个事实: 对于 $\alpha\in\Omega$, 只要 $\alpha\notin K$, 则 K 有一个 Ω- 实闭包 R, 使得 $\alpha\notin R$.

设 $\alpha\in\Omega$, 但 $\alpha\notin K$. 当 $\sigma(\alpha)\neq\alpha$ 时, 由引理 6.6.1(2) 知, 循环群 $\langle\sigma\rangle$ 的稳定域 R 是 K 的一个 Ω- 实闭包, 使得 $\alpha\notin R$. 下设 $\sigma(\alpha)=\alpha$. 此时有 $\tau\in\operatorname{Aut}(\Omega/K)$, 使得 $\tau(\alpha)\neq\alpha$. 若 $\tau\in\sigma\operatorname{Aut}(\Omega/K(\sqrt{-1}))$, 则 τ 是一个 2 阶元素. 由刚才的讨论知, K 有一个不包含 α 的 Ω- 实闭包. 若 $\tau\in\operatorname{Aut}(\Omega/K(\sqrt{-1}))$, 则 $\sigma\tau$ 的阶为 2. 由于 $\sigma\tau(\alpha)=\sigma(\tau(\alpha))\neq\sigma(\alpha)=\alpha$, 从而上面事实仍成立.

(4) $\Longrightarrow$ (1): 设 K 是 F 在 Ω 中的任意一个实扩张. 由叙述 (4) 知, K 是它的所有 Ω- 实闭包的交集. 由于每个 Ω- 实闭包都是 Pythagoras 域, 从而 K 是 Pythagoras 域. 因此, F 是相对 Ω 的遗传 Pythagoras 域. 证毕.

由上面定理中蕴含关系 “(1) $\Longrightarrow$ (2)” 的证明可看出, 如下结论成立.

推论 设 F 是一个实域, 则 F 是相对 Ω 的遗传 Pythagoras 域, 当且仅当 $\operatorname{Aut}(F\langle 2\rangle/F(\sqrt{-1}))$ 和 $\operatorname{Aut}(\Omega/F\langle 2\rangle)$ 都是 Abel 群.

遗传 Pythagoras 域还具有许多重要的其他性质, 感兴趣的读者可查阅文献 [9].

§6.7　具有变号性质的序域

在这一节中，我们讨论一类特殊的序域 —— 具有变号性质的序域. 在下面，将证明这样一个事实：一个序域 (F,P) 具有变号性质，当且仅当 F 是遗传欧氏域，或者 (F,P) 具有弱 Hilbert 性质.

定义 6.7.1　设 (F,P) 是一个序域，且 R 为它的实闭包. 称序域 (F,P) 具有变号性质，如果对于每个 $\alpha\in R$, α 在 F 上的极小多项式在 (F,P) 上是不定的.

首先，我们寻求一些充分条件，以保证具有实根的正定不可约多项式的存在.

命题 6.7.1　设 (F,P) 是一个序域，v 是 F 的一个与 P 相容的赋值，且 G_v 为 v 的值群. 若 $|G_v/2G_v|\geqslant 2$, 则存在一个不可约多项式 $f(x)\in F[x]$, 使得 $f(x)$ 在 (F,P) 上是正定的，而 $f(x)$ 在 (F,P) 的实闭包 R 中有根.

证明　由条件，可选取一个元素 $a\in P$, 使得 $v(a)<0$, 且 $v(a)\in G_v$, 但 $v(a)\notin 2G_v$. 令 α 是多项式 x^4-a 在 R 中的惟一正根，且记 $\beta=\alpha^2$, 显然 $\beta^2=a$. 再令 $\delta_1=\alpha+\beta$, 则易知 $\delta_2=\beta-\alpha$, $-\beta+\alpha\sqrt{-1}$ 和 $-\beta-\alpha\sqrt{-1}$ 都是 δ_1 在 F 上的共轭元. 注意到 $f(x)=(x-\delta_1)(x-\delta_2)(x+\beta-\alpha\sqrt{-1})(x+\beta+\alpha\sqrt{-1})=(x^2-a)^2-4ax-a\in F[x]$, 从而 $f(x)$ 是 δ_1 在 F 上的极小多项式. 根据定理 3.2.5, v 可以惟一地拓展为 R 的一个实赋值 w. 令 $h=v(a)$, 显然 $w(\pm\alpha)=\dfrac{1}{4}h>\dfrac{1}{2}h=w(\beta)$. 由此可知，$w(\delta_1)=w(\delta_2)=\min\{w(\alpha),w(\beta)\}=\dfrac{1}{2}h$. 由于 $0<_{R^2}\beta$, 从而由 w 与正锥 R^2 的相容性知，$\pm\alpha<_{R^2}\beta$, 即 $\beta\pm\alpha>_{R^2}0$. 设 $b\in F$, 假若 $(b-\delta_1)(b-\delta_2)\leqslant_{R^2}0$, 则有 $0\leqslant_{R^2}\delta_2\leqslant_{R^2}b\leqslant_{R^2}\delta_1$. 由 w 与正锥 R^2 的相容性知，$\dfrac{1}{2}h=w(\delta_1)\leqslant w(b)\leqslant w(\delta_2)=\dfrac{1}{2}h$. 从而 $\dfrac{1}{2}h=w(b)=v(b)\in G_v$, 矛盾. 因而，$(b-\delta_1)(b-\delta_2)>_{R^2}0$. 此外，$(b+\beta-\alpha\sqrt{-1})(b+\beta+\alpha\sqrt{-1})=(b+\beta)^2+\alpha^2>_{R^2}0$. 于是 $f(b)>_{R^2}0$, 即 $f(b)>_P 0$. 由 b 的任意性知，$f(x)$ 在 (F,P) 上是正定的. 证毕.

为证明下一个命题，我们需要如下引理：

引理 6.7.2　设 v 是域 F 的一个赋值，G_v 是 v 的值群，$g\in G_v$, 但 $g\notin pG_v$, 这里 p 是一个奇素数. 如果 K 是 F 的一个有限扩张，w 是赋值 v 在 K 上的一个拓展，那么存在一个正整数 r, 使得 $g\notin p^rG_w$, 这里 G_w 为 w 的值群.

证明　假若对于每个正整数 k, $g\in p^kG_w$, 则有 $h_k\in G_w$, 使得 $g=p^kh_k$, $k=1,2,\cdots$. 由于商群 G_w/G_v 是有限群，从而有相异的自然数 s 和 t, 使得 $h_s-h_t\in G_v$. 不妨设 $t<s$, 则 $g=p^sh_s=p^s(h_s-h_t)+p^{s-t}(p^th_t)=p^s(h_s-h_t)+p^{s-t}g\in pG_v$, 矛盾. 从而引理获证. 证毕.

命题 6.7.3　设 (F,P) 是一个序域，v 是 F 的一个与 P 相容的赋值，且 G_v 是 v 的值群，使得对于某个奇素数 p, $G_v\neq pG_v$. 如果 F 不是遗传欧氏域，则存在

一个不可约多项式 $f(x) \in F[x]$, 使得 $f(x)$ 在 (F,P) 上是正定的，而 $f(x)$ 在 (F,P) 的实闭包 R 中有根.

证明 由于 F 不是遗传欧氏域，从而由定理 6.3.1 知，有某个不可约多项式 $f(x) \in F[x]$, 使得 $f(x)$ 在 R 中至少有两个根. 设 α 是 $f(x)$ 在 R 中一个根，则由定理 2.3.8 知，正锥 P 在 $F(\alpha)$ 上至少有两个拓展. 从而 $R^2 \cap F(\alpha) \neq F(\alpha)^2$, 即有 $\beta \in R^2 \cap F(\alpha)$, 使得 $\beta \notin F(\alpha)^2$. 令 $K = F(\beta)$, 且 $Q = R^2 \cap K$, 则 (K,Q) 是序域 (F,P) 的一个有限序扩张， $\beta \in Q$, 但 $\beta \notin K^2$.

记 A_v 为 v 的赋值环，则 β 显然是环 A_v 上一个代数元. 从而有非零元 $d \in A_v$, 使得 $d\beta$ 在 A_v 上整. 此时， $d^2\beta$ 在 A_v 上整， $K = F(d^2\beta)$, 且 $d^2\beta \notin K^2$. 通过用 $d^2\beta$ 替代元素 β, 我们可进一步假定， β 在 A_v 上整.

由于 $G_v \neq pG_v$, 从而有 $a \in P$, 使得 $g := v(a) < 0$, 且 $g \notin pG_v$. 由定理 3.2.5 知， v 可拓展为 R 的一个实赋值 w. 令 G 是 K 的赋值 $w|_K$ 的值群，则由引理 6.7.2 知，有某个正整数 r, 使得 $g \notin p^rG$. 显然， F 上多项式 $x^{p^r} - a$ 在 R 中有惟一根 ξ, 且 $\xi >_{R^2} 0$. 注意到 $\xi \notin K$; 否则 $g = v(a) = w(\xi^{p^r}) = p^r w(\xi) \in p^rG$. 显然， ξ 在 K 上的极小多项式在 R 中只能有惟一根 ξ. 从而扩张次数 $m := [K(\xi):K]$ 为奇数. 令 η 是多项式 $x^2 - \beta$ 在 R 中的惟一正根，则 $[K(\eta):K] = 2$. 令 $L = K(\xi,\eta)$, 则显然有， $[L:K] = 2m$, 且 $L = F(\xi,\eta)$.

考虑 F 和 L 的所有形如 $F(\xi + n\eta)$ 的中间域，其中 $n \in \mathbb{N}$. 由于 F 和 L 之间只有有限个中间域，从而有相异的自然数 s 和 t, 使得 $F(\xi + s\eta) = F(\xi + t\eta)$. 此时可知， $L = F(\delta)$, 其中 $\delta = \xi + s\eta$.

设 σ 是 L 到 R 的任意一个 F- 嵌入，则由定理 2.3.8 可知， $\sigma(\xi) = \xi$. 此外, $\sigma(\beta) = \sigma(\eta)^2$ 是 β 在 F 上的极小多项式的一个正根. 注意到， $w \circ \sigma$ 是赋值 v 在 L 上的一个拓展，且 β 在 A_v 上整. 从而 $w \circ \sigma(\beta) \geqslant 0$, 即 $w(\sigma(\beta)) \geqslant 0$. 由此有 $w(\sigma(\eta)) = \frac{1}{2} w(\sigma(\beta)) \geqslant 0 > \frac{1}{p^r} g = w(\xi)$, 于是有

$$w(\sigma(\delta)) = w(\sigma(\xi) + s\sigma(\eta)) = w(\xi + s\sigma(\eta)) = w(\xi) = \frac{1}{p^r} g.$$

令 $f(x)$ 是 δ 在 F 上的极小多项式，则 $f(x)$ 的次数为偶数. 从而 $f(x)$ 在 R 中有偶数个根 $\delta_1 >_{R^2} \delta_2 >_{R^2} \cdots >_{R^2} \delta_{2k}$. 由上面讨论知， $w(\delta_i) = \frac{1}{p^r} g$, $i = 1, \cdots, 2k$. 由于 $\xi >_{R^2} 0$, 且对于 L 到 R 中每个 F- 嵌入 σ, $w(\xi) < w(\sigma(\eta)) = w(-s\sigma(\eta))$, 从而由 w 与 R^2 的相容性知， $-s\sigma(\eta) <_{R^2} \xi$, 即 $\sigma(\delta) >_{R^2} 0$. 由此可知， $\delta_{2k} >_{R^2} 0$. 假若对于某个 $b \in F$, $f(b) \leqslant_P 0$, 则必有 $0 <_{R^2} \delta_{2k} \leqslant_{R^2} b \leqslant_{R^2} \delta_1$. 再由 w 与 R^2 的相容性有 $\frac{1}{p^r} g = w(\delta_1) \leqslant w(b) = v(b) \leqslant w(\delta_{2k}) = \frac{1}{p^r} g$. 由此有， $g = p^r v(b) \in p^r G_v$, 矛盾. 因此， $f(x)$ 是命题所要求的一个不可约多项式. 证毕.

由上面两个命题，容易证明如下结果.

定理 6.7.4 设 (F,P) 是一个序域, v 是 F 的一个与 P 相容的赋值, 使得它的值群 G_v 不是可除群. 如果 (F,P) 具有变号性质, 则 F 是一个遗传欧氏域.

证明 由于 (F,P) 具有变号性质, 从而由命题 6.7.1 知, $G_v=2G_v$, 即 G_v 是 2- 可除的. 由所设知, G_v 不是可除群. 从而, 对于某个奇素数 p, $G_v\neq pG_v$. 根据命题 6.7.3, F 必为遗传欧氏域. 证毕.

下面, 我们将通过考察实赋值的剩余域来给出一些充分条件, 以保证具有实根的正定不可约多项式的存在.

命题 6.7.5 设 (F,P) 是一个序域, v 是 F 的一个与 P 相容的非浅显赋值. 如果 v 的剩余域 F_v 不是欧氏域, 那么存在一个不可约多项式 $f(x)\in F[x]$, 使得 $f(x)$ 在 (F,P) 上是正定的, 而 $f(x)$ 在 (F,P) 的实闭包 R 中有根.

证明 由命题 3.1.3 的推论知, P 在剩余域 F_v 上诱导出一个正锥 $\overline{P}$. 由于 F_v 不是欧氏域, 从而 $\overline{P}\neq F_v^2$. 于是有 $\bar{a}\in\overline{P}$, 其中 $a\in P\cap A_v$, 使得 $\bar{a}\notin F_v^2$. 显然, $a\notin M_v$, 且 $a\notin F^2$. 设 α 是多项式 x^4-a 在 R 中惟一正根, 且令 $\beta=\alpha^2$, 则 $a=\beta^2$. 此时, 易知 $[F(\beta):F]=[F(\alpha):F(\beta)]=2$. 由于 v 是一个非浅显赋值, 从而有非零元 $y\in P$, 使得 $v(y)>0$. 显然, $F(\alpha)=F(y\alpha)$. 类似于命题 6.7.1 的证明, 可证 $\beta+y\alpha$ 在 F 上的极小多项式 $f(x)$ 在 R 中只有两个根: $\delta_1=\beta+y\alpha$ 和 $\delta_2=\beta-y\alpha$. 记 w 是赋值 v 在 R 上惟一拓展的实赋值, 则 $w(\pm y\alpha)=w(\alpha)+w(y)=v(y)>0=w(\beta)$. 从而 $w(\delta_1)=w(\beta)=0$. 同样, $w(\delta_2)=0$. 由 w 与正锥 R^2 的相容性知, $\pm y\alpha<_{R^2}\beta$. 从而有 $0<_{R^2}\delta_2<_{R^2}\delta_1$. 假若对于某个 $b\in F$, $f(b)\leqslant_P 0$, 则必有 $0<_{R^2}\delta_2\leqslant_{R^2}b\leqslant_{R^2}\delta_1$. 由 w 与 R^2 的相容性有 $0=w(\delta_1)\leqslant w(b)\leqslant w(\delta_2)=0$. 从而 $w(b)=0$, 即 b 是赋值环 A_w 中可逆元. 设 $\leqslant$ 是 R 的惟一序 $\leqslant_{R^2}$ 在 w 的剩余域 F_w 上所诱导的序, 则有 $\bar{\delta}_2\leqslant\bar{b}\leqslant\bar{\delta}_1$. 注意到 $\bar{\delta}_1=\bar{\delta}_2=\bar{\beta}$, 从而 $\bar{\beta}=\bar{b}$, 即 $\beta-b\in M_w$. 此时有 $a-b^2=\beta^2-b^2=(\beta+b)(\beta-b)\in M_w\cap F=M_v$, 即有 $\bar{a}=a+M_v=(b+M_v)^2\in F_v^2$, 矛盾. 因而, $f(x)$ 在 (F,P) 上是正定的. 证毕.

命题 6.7.6 设 (F,P) 是一个序域, v 是 F 的一个与 P 相容的非浅显赋值. 如果 F 不是遗传欧氏域, 且 v 的剩余域 F_v 有一个奇次数的真扩张, 那么存在一个不可约多项式 $f(x)\in F[x]$, 使得 $f(x)$ 在 (F,P) 上是正定的, 而 $f(x)$ 在 (F,P) 的实闭包 R 中有根.

证明 设 w 是 v 在 R 上惟一拓展的实赋值. 由于 F_v 有一个奇次数的真扩张, 从而 $F_v[x]$ 中有一个首项系数为 1 的不可约多项式 $H(x)$, 使得 $H(x)$ 的次数为大于 1 的奇数. 于是, $A_v[x]$ 中有一个次数相同的首项系数为 1 的多项式 $h(x)$, 使得 $h(x)$ 在典型同态: $A_v[x]\longrightarrow F_v[x]$ 下的象恰为 $H(x)$. 设 $\alpha_1,\cdots,\alpha_s$ 是 $h(x)$ 在 R 中的全部根, 其中 s 为奇数. 注意到 $\alpha_1,\cdots,\alpha_s$ 在 A_v 上整, 从而 $\alpha_1,\cdots,\alpha_s\in A_w$. 显然, $\bar{\alpha}_i=\alpha_i+M_w$ 是 $H(x)$ 在 F_w 中的根, $i=1,\cdots,s$.

由于 F 不是遗传欧氏域, 从而可断言: F 有一个偶次数扩张 K, 使得 $K\subseteq R$.

事实上，当 $P \neq F^2$ 时，有 $a \in P$, 但 $a \notin F^2$. 令 α 是多项式 $x^2 - a$ 在 R 中一个根，且 $K = F(\alpha)$, 则 $K \subseteq R$, 且 $[K:F] = 2$. 当 $P = F^2$ 时，由定理 6.3.1 知，F 有一个偶次数实扩张 E. 令 Q 为 E 的任意一个正锥．由于 P 是 F 的惟一正锥，从而 (E, Q) 是序域 (F, P) 的一个有限序扩张．由实闭包的惟一性知，存在 E 到 R 的一个 F- 嵌入 σ. 令 $K = \sigma(E)$, 则 $K \subseteq R$, 且 $[K:F] = [E:F]$.

由本原元定理，$K = F(\beta)$. 不失一般性，可假定 β 在 A_v 上整．由于 v 是非浅显的，从而有非零元 $y \in P$, 使得 $v(y) > 0$. 此时有 $K = F(y\beta)$. 用 $y\beta$ 代替元素 β, 从而可进一步认定：$w(\beta) > 0$. 此时，对于 K 到 R 的每个 F- 嵌入 σ, $w(\sigma(\beta)) > 0$, 即 $\sigma(\beta) \in M_w$.

设 α 是 $h(x)$ 在 R 中一个根，且令 $L = F(\alpha, \beta)$, 则 $L \subseteq R$. 类似于命题 6.7.3 的证明，可得 $L = F(\delta)$, 这里 $\delta = \alpha + k\beta$, 其中 k 是一个自然数.

注意到，$[F(\alpha)(\beta):F(\alpha)][F(\alpha):F] = [K(\alpha):K][K:F]$, 其中 $[F(\alpha):F]$ 为奇数，$[K:F]$ 为偶数．从而 $[F(\alpha)(\beta):F(\alpha)]$ 是偶数．令 $g(x)$ 为 β 在 $F(\alpha)$ 上的极小多项式，则 $g(x)$ 的次数为偶数.

设 $f(x)$ 是 δ 在 F 上的极小多项式，且 Σ 是由 L 到 R 的所有 F- 嵌入组成的集合．显然，$f(x)$ 在 R 中的全部根恰为 $\{\sigma(\delta) \mid \sigma \in \Sigma\}$. 在集 Σ 上按如下方式规定一个二元关系 $\sim$: 对于 $\sigma_1, \sigma_2 \in \Sigma$, $\sigma_1 \sim \sigma_2$ 当且仅当 $\sigma_1(\alpha) = \sigma_2(\alpha)$. 显然，$\sim$ 是 Σ 上的一个等价关系．从而 $\Sigma = \Sigma_1 \cup \cdots \cup \Sigma_r$, 这里 $\Sigma_1, \cdots, \Sigma_r$ 是关于 $\sim$ 的全部相异的等价类．对于任意一个 Σ_i, 取定 $\sigma \in \Sigma_i$, 且令 $\tau = \sigma|_{F(\alpha)}$, 则 Σ_i 恰好是由 τ 所拓展的 L 到 R 的全部嵌入．因此，Σ_i 中的嵌入个数等于 $f^\tau(x)$ 在 R 中的根个数，这里 $f^\tau(x)$ 是 $f(x)$ 的全部系数通过 τ 作用后所得到的多项式．由于 $f^\tau(x)$ 的次数也为偶数，从而 $f^\tau(x)$ 在 R 中有偶数个根，即 Σ_i 中含有偶数个 F- 嵌入.

由上面的讨论知，$f(x)$ 在 R 上可分解如下：

$$f(x) = f_1(x) \cdots f_r(x)\phi(x),$$

其中 $f_i(x) = \prod_{\sigma \in \Sigma_i} (x - \sigma(\delta))$, $i = 1, \cdots, r$, $\phi(x)$ 是 $R[x]$ 中首项系数为 1 的多项式，且 $\phi(x)$ 在 R 中不再有根．显然，对于每个 $c \in F$, $\phi(c) >_P 0$. 假若对于某个 $b \in F$, $f(b) \leqslant_P 0$, 则必有某个 j, $1 \leqslant j \leqslant r$, 使得 $f_j(b) \leqslant_{R^2} 0$. 注意到，Σ_j 中含有偶数个 F- 嵌入．从而有 $\sigma_1, \sigma_2 \in \Sigma_j$, 使得 $\sigma_1(\delta) \leqslant_{R^2} b \leqslant_{R^2} \sigma_2(\delta)$. 令 $\sigma_1(\alpha) = \alpha_t$, $1 \leqslant t \leqslant s$, 则 $\alpha_t + k\sigma_1(\beta) \leqslant_{R^2} b \leqslant_{R^2} \alpha_t + k\sigma_2(\beta)$. 从而，$0 \leqslant_{R^2} b - \alpha_t - k\sigma_1(\beta) \leqslant_{R^2} k\sigma_2(\beta) - k\sigma_1(\beta) \in M_w$. 由于 M_w 关于序 $\leqslant_{R^2}$ 是凸的，从而 $b - \alpha_t - k\sigma_1(\beta) \in M_w$, 即有 $b - \alpha_t \in M_w$. 由此有 $\bar{\alpha}_t = \bar{b} \in F_v$, 矛盾于 $H(x)$ 在 F_v 上的不可约性．因此，$f(x)$ 在 (F, P) 上是正定的．证毕.

现在，我们可以给出具有变号性质的序域的如下刻画.

定理 6.7.7　序域 (F, P) 具有变号性质，当且仅当 F 是遗传欧氏域，或者 (F, P)

具有弱 Hilbert 性质.

证明 设 R 是序域 (F,P) 的实闭包.

充分性：设 $\alpha\in R$, 且 $f(x)$ 是 α 在 F 上的极小多项式. 当 F 是遗传欧氏域时，由定理 6.3.1 知， $f(x)$ 在 R 中只有惟一根 α. 根据引理 1.2.2, 有 $M\in F$, 使得 $-M<_{R^2}\alpha<_{R^2}M$. 此时，显然有 $f(M)f(-M)<_P 0$. 当 (F,P) 具有弱 Hilbert 性质时，由定理 4.2.4 知， F 在 R 中是稠密的. 由于 α 是 $f(x)$ 在 R 中的单根，从而 $f(x)$ 在 R 上可取正值和负值. 于是 $f(x)$ 在 (F,P) 上也可取正值和负值. 从而充分性获证.

必要性：设 (F,P) 具有变号性质，而 F 不是遗传欧氏域. 若 P 是一个阿基米德正锥，则 (F,P) 显然具有弱 Hilbert 性质. 现设 P 不是阿基米德正锥，且 v 是 F 的任意一个与 P 相容的非浅显赋值. 由定理 6.7.4 知， v 的值群 G_v 是可除的. 此外，由命题 6.7.5 和命题 6.7.6 知， v 的剩余域 F_v 是一个欧氏域，且 F_v 没有奇次数的真扩张. 由定理 2.1.3 可知， F_v 是一个实闭域. 根据定理 4.5.4, (F,P) 具有弱 Hilbert 性质. 定理获证. 证毕.

§6.8 满足 Rolle 定理的序域

在 §2.1 中，我们证明了，实闭域满足关于多项式的 Rolle 定理，参见定理 2.1.7. 在本节中，满足 Rolle 定理的序域将被刻画. 本节的结果表明，满足 Rolle 定理的序域是一类较实闭域更为广泛的序域.

定义 6.8.1 称一个序域 $(F,\leqslant)$ 满足 Rolle 定理，如果对于每个在 F 中有根 a 和 b 的多项式 $f(x)$, 其中 $a<b$, 微商 $f'(x)$ 在 F 中有根 c, 使得 $a<c<b$.

为刻画满足 Rolle 定理的序域，我们需要赋值论中如下事实，这一事实可见于一般的赋值论专著中，比如参见文献 [76] 中推论 20.23.

命题 6.8.1 设 v 是域 F 的一个 Hensel 赋值，且 v 的剩余域 F_v 的特征为零. 如果 w 是 v 在 F 的一个有限扩张 K 上的惟一拓展，那么

$$[K:F]=[G_w:G_v][F_w:F_v],$$

这里 G_v 和 G_w 分别为 v 和 w 的值群， F_w 为 w 的剩余域.

借助于命题 6.8.1, 我们可刻画满足 Rolle 定理的序域如下.

定理 6.8.2 对于一个序域 $(F,\leqslant)$, 下列叙述是等价的：

(1) $(F,\leqslant)$ 满足 Rolle 定理;

(2) 若 $f(x)\in B[x]$, 且 β 是 $f^{\pi}(x)$ 在 $\mathbb{R}$ 中的一个奇重数的根，则有 $\alpha\in B$, 使得 $f(\alpha)=0$, 且 $\pi(\alpha)=\beta$, 这里 π 是关于 $\leqslant$ 的典型 $\mathbb{R}$- 值位， $B=A(\mathbb{Q},\leqslant)$ 是位 π 的赋值环.

(3)F 有一个 Hensel 赋值 v, 使得剩余域 F_v 是实闭域，且值群 G_v 是奇可除的，即对于每个正奇数 m, $mG_v = G_v$.

证明 (1) $\Longrightarrow$ (2): 由所设， $f^\pi(x)$ 可写为

$$f^\pi(x) = \sum_{i=m}^{n} s_i(x-\beta)^i \in \mathbb{R}[x],$$

这里 m 为奇数，且 $s_m \neq 0$. 显然，至少有一个 $d \in B$, 使得 $\pi(d) \neq \beta$. 必要时用 $(x-d)f(x)$ 代替 $f(x)$ 来进行讨论，从而可假定对于某个偶数 t, $s_t \neq 0$. 同时，可选取 t 是使得 $s_t \neq 0$ 的最小偶数.

对于任意正数 ϵ, 定积分

$$a_\epsilon := \int_{\beta-\epsilon}^{\beta+\epsilon} f^\pi(x)\,\mathrm{d}x = \int_{-\epsilon}^{\epsilon} \sum_{i=m}^{n} s_i u^i\,\mathrm{d}u = 2(t+1)^{-1}s_t\epsilon^{t+1} + \epsilon^{t+3}\eta(\epsilon),$$

其中 $\eta(x) \in \mathbb{R}[x]$.

同样有

$$b_\epsilon := \int_{\beta-\epsilon}^{\beta+\epsilon} (x-\beta)f^\pi(x)\,\mathrm{d}x = 2(m+2)^{-1}s_m\epsilon^{m+2} + \epsilon^{m+4}\xi(\epsilon),$$

其中 $\xi(x) \in \mathbb{R}[x]$.

注意到 $t \geqslant m+1$. 从而当 ϵ 趋于零时， $\dfrac{b_\epsilon}{a_\epsilon}$ 趋于 ∞ 或 $\dfrac{s_m}{s_t}$, 且 a_ϵ 不可能为零. 因而，当正数 ϵ 充分小时，

$$\epsilon < \left|\frac{b_\epsilon}{a_\epsilon}\right| = \left|\beta - \frac{c_\epsilon}{a_\epsilon}\right|,$$

其中 $c_\epsilon = \int_{\beta-\epsilon}^{\beta+\epsilon} xf^\pi(x)\,\mathrm{d}x$.

这样，存在有理数 q 和 r, 使得 $\beta-\epsilon < q < \beta < r < \beta+\epsilon$, 且 $\left|\beta - \dfrac{\bar{c}}{\bar{a}}\right| > \epsilon$, 这里 $\bar{a} := \int_q^r f^\pi(x)\,\mathrm{d}x \neq 0$, $\bar{c} = \int_q^r xf^\pi(x)\,\mathrm{d}x$.

由于 $\mathbb{Q} \subseteq B$, 从而有 $g(x)$, $h(x) \in B[x]$, 使得 $g'(x) = f(x)$, $h'(x) = xf(x)$. 令 $a = g(r) - g(q)$, 且 $c = h(r) - h(q)$, 则易知， $\pi(a) = \bar{a}$, 且 $\pi(c) = \bar{c}$. 这表明 $a, c \in B$, 且 a 是 B 中可逆元. 此时， $\pi\left(\dfrac{c}{a}\right) = \dfrac{\bar{c}}{\bar{a}}$.

考察多项式

$$\varPhi(x) = \big(h(x) - h(q)\big) - \frac{c}{a}\big(g(x) - g(q)\big) \in B[x].$$

显然， $\varPhi(q) = \varPhi(r) = 0$. 由叙述 (1) 知，有 $\alpha \in F$, 使得 $q < \alpha < r$, 且 $\varPhi'(\alpha) = 0$, 即 $f(\alpha)\left(\alpha - \dfrac{c}{a}\right) = 0$. 假若 $\alpha = \dfrac{c}{a}$, 则 $\pi(\alpha) = \dfrac{\bar{c}}{\bar{a}}$. 由位 π 与序 $\leqslant$ 的相容性知， $q \leqslant \pi(\alpha) \leqslant r$, 即有 $\beta-\epsilon < \dfrac{\bar{c}}{\bar{a}} < \beta+\epsilon$, 矛盾. 因而 $f(\alpha) = 0$. 注意到 $\alpha \in A(\mathbb{Q}, \leqslant) = B$,

从而 $f^{\pi}(\pi(\alpha))=0$. 由于 $|\pi(\alpha)-\beta|<\epsilon$, 其中 ϵ 可取充分小正数，从而 $\pi(\alpha)=\beta$.

(2) $\Longrightarrow$ (3). 由叙述 (2), 可取 v 为赋值环 $B=A(\mathbb{Q},\leqslant)$ 所确定的实赋值. 此时，剩余域 $F_v=\pi(B)\subseteq\mathbb{R}$, 这里 π 是关于序 $\leqslant$ 的典型 $\mathbb{R}$- 值位. 设 $\beta\in\mathbb{R}$ 是 F_v 上的一个代数元，则有一个首项系数为 1 的不可约多项式 $f(x)\in B[x]$, 使得 $f^{\pi}(x)\in F_v[x]$, 且 $f^{\pi}(x)$ 是 β 在 F_v 上的极小多项式. 由叙述 (2) 知，有 $\alpha\in F$, 使得 $\beta=\pi(\alpha)\in F_v$. 因而，F_v 在 $\mathbb{R}$ 中是代数闭的. 根据命题 2.1.5, F_v 是实闭域. 现设 λ 是值群 G_v 中任意一个大于零的元素，则有 $a\in M_v$, 使得 $\lambda=v(a)$. 由叙述 (2) 可知，对于任意正奇数 m, 多项式 x^m-a 在 F 中有根 α. 此时，$\lambda=v(\alpha^m)=mv(\alpha)\in mG_v$, 这表明 G_v 是奇可除的. 此外，将叙述 (2) 与命题 3.4.1(1) 结合起来可知，v 是 F 的一个 Hensel 赋值.

(3) $\Longrightarrow$ (1): 设 $f(x)\in F[x]$, 且 a 和 b 是 $f(x)$ 在 F 中两个根，其中 $a<b$. 通过用 $f((b-a)x+a)$ 来代替 $f(x)$, 可假定 $a=0$, 且 $b=1$. 此外，可进一步假定 $f(x)\in A_v[x]$, 且 $f(x)$ 在自然同态: $A_v[x]\longrightarrow F_v[x]$ 下的象 $\bar{f}(x)$ 不是零多项式. 由所设，F_v 是一个实闭域，从而 F_v 有惟一序. 显然，$\bar{f}(0)=\bar{f}(1)=0$. 由引理 2.4.2 可知，微商 $\bar{f}'(x)$ 在 F_v 的开区间 $]0,1[$ 中必有一个奇重数的根 β. 从而有 $\bar{f}'(x)=(x-\beta)^m\psi(x)$, 这里 m 为奇数，$\psi(x)\in F_v[x]$, 且 $\psi(x)$ 与 $(x-\beta)^m$ 互素. 由 Hensel 引理 (命题 3.4.1(1)) 知，$f'(x)$ 在 $A_v[x]$ 中有一个次数为 m 的因式 $g(x)$, 使得 $\bar{g}(x)=(x-\beta)^m$. 于是 $g(x)$ 在 $F[x]$ 中至少有一个奇次数的不可约因式 $p(x)$. 令 α 是 $p(x)$ 在 $(F,\leqslant)$ 的实闭包 R 中一个根，则由定理 3.2.4 知，v 可惟一地拓展为 $F(\alpha)$ 的一个实赋值 w. 由命题 6.8.1 知，$[F(\alpha):F]=[G_w:G_v][F_w:F_v]$. 注意到 F_v 是实闭域，从而 $F_w=F_v$, 即 $[F_w:F_v]=1$. 又由于 G_v 是奇可除的，从而 $[G_w:G_v]$ 是 2 的一个方幂. 但 $[F(\alpha):F]$ 为奇数，因而必有 $[G_w:G_v]=2^0=1$. 于是 $[F(\alpha):F]=1$, 即 $\alpha\in F$. 注意到，$g(x)$ 的首项系数是赋值环 A_v 中的可逆元，从而 α 在 A_v 上整. 由于 A_v 在 F 中是整闭的，从而 $\alpha\in A_v$. 由此有 $\bar{\alpha}=\alpha+M_v=\beta$. 由于 $0<_{F_v^2}\bar{\alpha}=\beta<_{F_v^2}1$, 且 $\leqslant_{F_v^2}$ 是 $\leqslant$ 在 F_v 上所诱导的序，从而 $0<\alpha<1$. 显然，$f'(\alpha)=0$. 因此，$(F,\leqslant)$ 满足 Rolle 定理. 证毕.

推论 1 若域 F 关于某个序满足 Rolle 定理，则域 F 关于它的每个序都满足 Rolle 定理.

证明 由于定理 6.8.2 中叙述 (3) 不涉及域 F 的序，从而推论 1 成立. 证毕.

推论 2 一个阿基米德序域 $(F,\leqslant)$ 满足 Rolle 定理，当且仅当 F 是实闭域.

证明 充分性由定理 2.1.7 可知. 若 $(F,\leqslant)$ 满足 Rolle 定理，则由定理 6.8.2 知，F 有一个剩余域为实闭域的 Hensel 赋值 v. 由定理 3.4.5 知，v 与 $\leqslant$ 相容. 由于 $\leqslant$ 是阿基米德序，从而 v 是浅显赋值，即 F 为 v 的剩余域. 因此，F 为实闭域. 证毕.

推论 3 若序域 $(F,\leqslant)$ 满足 Rolle 定理，则 F 是一个遗传 Pythagoras 域.

证明 由定理 6.8.2 知, F 有一个 Hensel 赋值 v, 使得剩余域 F_v 是实闭域. 设 K 是 F 的任意一个实代数扩张, 且令 Q 为 K 的任意一个正锥. 由定理 3.4.5 知, v 与 $Q\cap F$ 相容. 再根据定理 3.2.4 知, v 可拓展为 K 的一个实赋值 w. 由于 w 的剩余域 F_w 是 F_v 的实代数扩张, 且 F_v 为实闭域, 从而 $F_w = F_v$, 即 F_w 为实闭域. 此外, w 显然也是 K 的 Hensel 赋值.

设 a 和 b 都是域 K 中非零元, 且 $w(a) \leqslant w(b)$, 则 $c := ba^{-1} \in A_w$. 考察多项式 $f(x) = x^2 - 1 - c^2 \in A_w[x]$, 则 $f(x)$ 在自然同态: $A_w[x] \longrightarrow F_w[x]$ 下的象为 $\bar{f}(x) = x^2 - \bar{1} - \bar{c}^2$. 由于 $\bar{1} + \bar{c}^2 \in F_w^2$, 从而有 $\beta \in F_w$, 使得 $\bar{1} + \bar{c}^2 = \beta^2$. 由此有 $\bar{f}(x) = (x+\beta)(x-\beta)$, 其中 $x+\beta$ 与 $x-\beta$ 互素. 由 Hensel 引理可知, $f(x)$ 在 A_w 中有根 d. 此时有 $a^2 + b^2 = a^2(1+c^2) = (ad)^2 \in K^2$. 这表明: K 是一个 Pythagoras 域. 根据定义 6.6.1 知, F 是一个遗传 Pythagoras 域. 证毕.

根据定理 6.8.2, 我们很容易构造一个并非实闭域但满足 Rolle 定理的序域如下:

例 设 G 是由所有这样的有理数 $\dfrac{m}{n}$ 组成的加法群, 其中 m 为整数, n 为奇数. 对于有理数之间通常的大小关系, G 是一个奇可除的序群.

考虑系数为实数而指数在 G 中的形式幂级域 $\mathbb{R}((G))$. 正如 §5.7 的例 2 中所说, 域 $\mathbb{R}((G))$ 有一个自然赋值 v, 使得 v 是 Hensel 的, 且 v 的剩余域和值群分别为 $\mathbb{R}$ 和 G. 根据定理 6.8.2 可知, 域 $\mathbb{R}((G))$ 关于它的每个序都满足 Rolle 定理.

然而, 根据定理 3.4.10 知, $\mathbb{R}((G))$ 不是实闭域, 因为 v 的值群 G 不是 2- 可除的.

§6.9 完 全 序 域

在这一节中, 我们考虑一类称作完全域的序域. 本节将指出: 任意一个序域都有一个完全的序扩张, 且在同构意义下, 这样一个完全的序扩张是惟一的.

定义 6.9.1 一个序域 (F,P) 称作是完全的, 如果对于 (F,P) 的任意一个真序扩张 (K,Q), F 关于由 Q 所诱导的区间拓扑在 K 中不是稠密的. 此时, 亦称序域 $(F,\leqslant)$ 是完全序域, 这里 $\leqslant$ 是正锥 P 的对应序.

完全序域的一个典型例子是 $(\mathbb{R},\leqslant)$, 其中 $\leqslant$ 为实数域 $\mathbb{R}$ 上通常的大小关系. 事实上, 若 $(K,\leqslant_K)$ 是 $(\mathbb{R},\leqslant)$ 的一个真序扩张, 则有 $y \in K$, 使得 $y \notin \mathbb{R}$. 令 $D = \{r \in \mathbb{R} \mid r <_K y\}$. 当 $D = \mathbb{R}$ 时, 显然 $\mathbb{R}$ 中没有元素在 y 和 $y+1$ 之间. 当 $D = \emptyset$ 时, $\mathbb{R}$ 中没有元素在 $y-1$ 和 y 之间. 当 $D \neq \mathbb{R}$ 且 $D \neq \emptyset$ 时, D 是一个在 $\mathbb{R}$ 中有上界的非空子集. 从而, D 有上确界 $s \in \mathbb{R}$. 易知, $y-s$ 关于序 $\leqslant_K$ 是在 $\mathbb{R}$ 上的无限小元素. 此时, $\mathbb{R}$ 中不可能有元素在 $y-s$ 和 $2(y-s)$ 之间. 因此, $(\mathbb{R},\leqslant)$ 是完全序域.

在 §4.2 中，为了建立 McKenna 定理，我们在序域的实闭包中引进了“极限元”这一概念. 实际上，“极限元”这一概念可引入到序域的任意一个序扩张之中. 设 (K,Q) 是序域 (F,P) 的一个序扩张. K 中一个元素 α 称作是关于 F 的极限元，若对于任意正元素 $\delta \in P$, 总有 $a \in F$, 使得 $\alpha <_Q a <_Q \alpha + \delta$.

关于极限元，我们可建立如下引理.

引理 6.9.1 设 (K,Q) 是序域 (F,P) 的一个序扩张，且 Q 是在 F 上的阿基米德正锥，则 K 中所有关于 F 的极限元组成一个包含 F 的子域 $\hat{F}$, 且对于由正锥 $Q \cap \hat{F}$ 所确定的区间拓扑，F 在 $\hat{F}$ 中稠密.

证明 由类似于引理 4.2.2 的证明可知，$\hat{F}$ 是 K 的一个包含 F 的子域.

设 $\alpha, \beta \in \hat{F}$, 且 $\alpha <_{\hat{P}} \beta$, 这里 $\hat{P} = Q \cap \hat{F}$. 由于 Q 是在 F 上的阿基米德正锥，从而有正元素 $\delta \in P$, 使得 $(\beta - \alpha)^{-1} <_Q \delta$, 即 $\delta^{-1} <_Q \beta - \alpha$. 此外，由于 α 是关于 F 的极限元，从而有 $a \in F$, 使得 $\alpha <_Q a <_Q \alpha + \delta^{-1}$. 此时有，$\alpha <_{\hat{P}} a <_{\hat{P}} \beta$. 因此，$F$ 在 $\hat{F}$ 中稠密. 证毕.

设 (F,P) 是一个序域. 按照定义 2.6.1, F 关于 P 的一个分割是域 F 的一个子集 D, 它满足这样一个条件：对于 $a \in F$, 只要有 $d \in D$, 使得 $a <_P d$, 总有 $a \in D$. F 关于 P 的一个分割 D 称作超越的，如果 D 是 F 的一个非空的真子集，使得 D 中没有最大元，而 $F \setminus D$ 中没有最小元.

为刻画完全的序域，我们还需要如下定义.

定义 6.9.2 设 (F,P) 是一个序域，D 是 F 关于 P 的一个分割. 称 D 在平移下变化，若对于每个非零 $a \in F$, $a + D \neq D$, 这里 $a + D := \{a + d \mid d \in D\}$.

显然，若域 F 关于其正锥 P 的一个分割 D 在平移下变化，则 D 必是 F 的一个非空真子集.

现在，我们可以给出完全序域的如下刻画.

定理 6.9.2 一个序域 (F,P) 是完全的，当且仅当 F 关于 P 的每个在平移下变化的分割都不是超越的.

证明 充分性：设 (F,P) 不是完全的，则 (F,P) 有一个真序扩张 (K,Q), 使得对于由 Q 所确定的区间拓扑，F 在 K 中稠密. 取 $z \in K$, 使得 $z \notin F$. 令 $D = \{a \in F \mid a \leqslant_Q z\}$. 对于任意正元素 δ, 由 F 在 K 中的稠密性知，有 $b, c \in F$, 使得 $z - \delta <_Q b <_Q z <_Q c <_Q z + \delta$. 由此可知，$b \in D$ 但 $b \notin -\delta + D$, 而 $c \in \delta + D$ 但 $c \notin D$. 因此，D 在平移下变化. 假若 D 中有最大元素 d, 则 $d <_Q z$. 由 F 在 K 中的稠密性知，有 $a \in F$, 使得 $d <_Q a <_Q z$. 此时有 $a \in D$, 矛盾于 d 在 D 中的最大性. 同样可证，$F \setminus D$ 中没有最小元素. 这表明 D 是超越的. 从而充分性获证.

必要性：设 D 是 F 的一个关于 P 的超越分割，且 D 在平移下是变化的. 设

R 是序域 (F,P) 的实闭包，且令 $D_R=\{\alpha\in R \mid 有\ d\in D, 使得\ \alpha\leqslant_{R^2} d\}$. 容易验证：$D_R$ 是 R 的一个分割，使得 $D\subseteq D_R$, $F\setminus D\subseteq R\setminus D_R$, 且 D_R 中没有最大元素. 现分如下两种情况讨论：

(1)D_R 不是超越的. 此时，$R\setminus D_R$ 中有最小元素 β. 显然，$\beta\notin F$. 对于任意正元素 $\delta\in P$, $\beta-\delta\notin R\setminus D_R$, 即 $\beta-\delta\in D_R$. 从而有 $d\in D$, 使得 $\beta-\delta\leqslant_{R^2} d$. 显然，$d<_{R^2}\beta$. 由此有 $\beta\leqslant_{R^2} d+\delta<_{R^2}\beta+\delta$. 这表明. β 是关于 F 的极限元. 由定理 1.4.2 知，R 的惟一正锥 R^2 在 F 上是阿基米德的. 根据引理 6.9.1 可知，域 $F(\beta)$ 中每个元素都是关于 F 的极限元，且对于由正锥 $R^2\cap F(\beta)$ 所确定的区间拓扑，F 在 $F(\beta)$ 中稠密.

(2)D_R 是超越的. 此时，由定理 2.6.3 知，D_R 确定单超越扩张 $F(t)$ 的一个正锥 Q, 使得 $P\subseteq Q$, Q 在 F 上是阿基米德的，且对于每个 $d\in D$ 以及 $e\in F\setminus D$, $d<_Q t<_Q e$. 设 $\delta\in P$ 且 $\delta\neq 0$. 假若对于每个 $d\in D$, $d<_Q t-\delta$, 则 $d+\delta<_Q t$. 从而 $d+\delta\notin F\setminus D$, 即 $d+\delta\in D$. 于是 $\delta+D\subseteq D$, 必然 $\delta+D=D$, 与所设矛盾. 从而有某个 $d_1\in D$, 使得 $t-\delta<_Q d_1$. 由于 $d_1<_Q t$, 从而有 $t<_Q d_1+\delta<_Q t+\delta$, 其中 $d_1+\delta\in F$. 这表明. t 是关于 F 的极限元. 由引理 6.9.1 可知，对于由 Q 所确定的区间拓扑，F 在 $F(t)$ 中稠密.

综合上面两种情况可知，(F,P) 不是完全的. 从而必要性获证. 证毕.

对于序域 (F,P), 用 $\mathcal{D}$ 表示由 F 关于 P 的所有分割组成的集合，$Z=\{z_D\mid D\in\mathcal{D}\}$ 是一个指标集为 $\mathcal{D}$ 的未定元集. 令 $F^*=F(Z)$ 是域 F 的以 Z 为超越基的纯超越扩张，且 U 是在乘法么半群 F^* 中由 P 中元素以及全部如下形式的元素生成的子么半群：

(1) z_D-d, 其中 $D\in\mathcal{D}$, $d\in D$;

(2) $e-z_D$, 其中 $D\in\mathcal{D}$, $e\in F\setminus D$.

由此可得 F^* 的如下子集：

$$T^*=\left\{\sum_{i=1}^{n}u_i\alpha_i^2\mid n\in\mathbb{N}, u_i\in U, \alpha_i\in F^*, i=1,\cdots,n\right\}.$$

引理 6.9.3 所设同上，则 T^* 是域 F^* 的一个亚正锥.

证明 显然，$T^*+T^*\subseteq T^*$, $T^*\cdot T^*\subseteq T^*$, 且 $F^{*2}\subseteq T^*$. 由定义 1.1.4 知，只须证明 $-1\notin T^*$. 假若 $-1\in T^*$, 则有

$$-1=\sum_{i=1}^{n}u_i\alpha_i^2,$$

其中 $n\in\mathbb{N}$, $u_i\in U$, $\alpha_i\in F^*$, $i=1,\cdots,n$.

由域 F^* 的构造知，存在有限个相异的 $D_1, \cdots, D_m \in \mathcal{D}$, 其中 $m \geqslant 0$, 使得 u_i, $\alpha_i \in F(z_{D_1}, \cdots, z_{D_m})$, $i = 1, \cdots, n$. 由非负整数的良序性，存在一个最小的非负整数 m, 使得上面的等式以及所有关系式都成立. 注意到， $m > 0$; 否则 $u_i \in P$ 且 $\alpha_i \in F$, $i = 1, \cdots, n$, 此将导致矛盾： $-1 = \sum_{i=1}^{n} u_i\alpha_i^2 \in P$. 由 U 的构造可知，诸元素 $u_1, \cdots, u_n$ 只涉及有限个如下形式的元素：(1)$z_{D_m} - d_j$, 其中 $d_j \in D_m$, $j = 1, \cdots, r$; (2)$e_k - z_{D_m}$, 其中 $e_k \in F \setminus D_m$, $k = 1, \cdots, s$. 显然，存在 F 中一个开区间 $]b, c[_P$, 使得 $d_j <_P b <_P c <_P e_k$, $j = 1, \cdots, r$; $k = 1, \cdots, s$. 设 $\alpha_i = \dfrac{f_i}{g_i}$, 其中 f_i, $g_i \in F[z_{D_1}, \cdots, z_{D_m}]$, 且 $g_i \neq 0$, $i = 1, \cdots, n$. 由于开区间 $]b, c[_P$ 中有无限多个元素，从而有 $a \in]b, c[_P$, 使得通过代换 $z_{D_m} = a$, 多项式 $g_1, \cdots, g_n$ 的值均不为零. 记 w_i 和 β_i 分别是 u_i 和 α_i 通过代换 $z_{D_m} = a$ 后所得的值， $i = 1, \cdots, n$. 显然， $w_i \in U \cap F(z_{D_1}, \cdots, z_{D_{m-1}})$, 且 $\beta_i \in F(z_{D_1}, \cdots, z_{D_{m-1}})$. 由上面的等式有 $-1 = \sum_{i=1}^{n} w_i\beta_i^2$; 矛盾于 m 的最小性. 因而， $-1 \notin T^*$. 证毕.

由引理 6.9.3 和定理 1.1.2 的推论知，域 F^* 至少有一个包含 T^* 的正锥. 任意取定 F^* 的这样一个正锥，且记作 P^*. 显然， (F^*, P^*) 是 (F, P) 的一个序扩张.

现在，我们可以建立如下重要的定理.

定理 6.9.4 设 (F, P) 是一个序域，则 (F, P) 有一个完全的序扩张 $(\hat{F}, \hat{P})$, 使得对于由 $\hat{P}$ 所确定的区间拓扑， F 在 $\hat{F}$ 中稠密.

证明 所求的完全序扩张 $(\hat{F}, \hat{P})$ 将按如下步骤构造：

(1) 按照上面的方式，构造序域 (F, P) 的序扩张 (F^*, P^*).

(2) 令 $A = A(F, P^*)$, 则由 §3.2 中讨论， A 是 F^* 的一个与正锥 P^* 相容的赋值环. 此外，用 K 表示实赋值环 A 的剩余域. 根据命题 3.1.3 的推论， P^* 在 K 上诱导出一个正锥 Q, 使得 $Q = \{\bar{a} = a + M \mid a \in P^* \cap A\}$, 这里 M 为 A 的极大理想. 由定理 3.2.2 的推论 2 知，若认定 $F + M/M = F$, 则 (K, Q) 是序域 (F, P) 的一个序扩张，且 Q 是在子域 F 上的阿基米德正锥.

(3) 最后，设 $\hat{F}$ 是 K 中所有关于 F 的极限元组成的集合，且令 $\hat{P} = Q \cap \hat{F}$. 由引理 6.9.1 可知， $(\hat{F}, \hat{P})$ 是序域 (F, P) 的一个序扩张，且对于由 $\hat{P}$ 所确定的区间拓扑， F 在 $\hat{F}$ 中稠密.

下面证明序扩张 $(\hat{F}, \hat{P})$ 的完全性.

设 (E, Q_E) 是 $(\hat{F}, \hat{P})$ 的任意序扩张，且对于由 Q_E 所确定的区间拓扑， $\hat{F}$ 在 E 中稠密. 此时，显然 F 在 E 中稠密. 设 $z \in E$, 且令 $D = \{d \in F \mid d \leqslant_{Q_E} z\}$, 则 D 是 F 关于 P 的一个分割. 由序扩张 (F^*, P^*) 的构造知，有 $z_D \in F^*$, 使得对于每个 $d \in D$ 以及每个 $e \in F \setminus D$, $d <_{P^*} z_D <_{P^*} e$. 对于任意正元素 $\delta \in P$, 由 F 在 E 中的稠密性可知，有 $d_1, e_1 \in F$, 使得 $z - \delta <_{Q_E} d_1 <_{Q_E} z <_{Q_E} e_1 <_{Q_E} z + \delta$. 此时 $d_1 \in D$,

而 $e_1\in F\setminus D$. 因而, $d_1<_{P^*}z_D<_{P^*}e_1$. 这表明 $z_D\in A$, 从而 $\bar{z}_D=z_D+M\in K$. 由于 Q 是由 P^* 所诱导的, 从而 $\bar{z}_D\leqslant_Q e_1$. 注意到 $e_1-\delta<_{Q_E}z$, 即有 $e_1-\delta\in D$. 于是 $e_1-\delta<_{P^*}z_D$, 进而 $e_1-\delta\leqslant_Q\bar{z}_D$. 这样, 我们有 $\bar{z}_D\leqslant_Q e_1\leqslant_Q\bar{z}_D+\delta$. 由 δ 的任意性知, $\bar{z}_D\in\hat{F}$. 假若 $z<_{Q_E}\bar{z}_D$, 则由 F 在 E 中的稠密性知, 有 $b\in F$, 使得 $z<_{Q_E}b<_{Q_E}\bar{z}_D$. 注意到 $b\in F\setminus D$, 从而有 $z_D<_{P^*}b$. 由此有 $\bar{z}_D\leqslant_Q b$, 即有 $\bar{z}_D\leqslant_{Q_E}b$, 矛盾. 因而, $\bar{z}_D\leqslant_{Q_E}z$. 同理可证 $z\leqslant_{Q_E}\bar{z}_D$. 于是 $z=\bar{z}_D\in\hat{F}$. 因此, $E=\hat{F}$. 这表明序域 $(\hat{F},\hat{P})$ 是完全的. 证毕.

满足上面定理中条件的完全序扩张 $(\hat{F},\hat{P})$ 称作序域 (F,P) 的一个完全化. 至于完全化的惟一性, 我们可建立如下定理.

定理 6.9.5 设 (F,P) 是一个序域, 则在保序 F- 同构的意义下, (F,P) 的完全化是惟一的.

证明 设 $(\hat{F},\hat{P})$ 和 (K,Q) 均为序域 (F,P) 的完全化. 下面将指出: 存在 (K,Q) 到 $(\hat{F},\hat{P})$ 的一个保序 F- 同构.

对于 $x\in K$, 令 $D_x=\{d\in F\mid d\leqslant_Q x\}$. 易知, D_x 是 F 关于 P 的一个分割, 且 D_x 在平移下是变化的. 再令 $\widehat{D}_x=\{\alpha\in\hat{F}\mid 有\ d\in D_x, 使得\ \alpha<_{\hat{P}}d\}$, 则由 F 在 $\hat{F}$ 中的稠密性知, $\widehat{D}_x$ 是 $\hat{F}$ 关于 $\hat{P}$ 的一个在平移下变化的分割. 由于 $(\hat{F},\hat{P})$ 是完全的序域, 从而由定理 6.9.2 知, $\widehat{D}_x$ 不是超越的. 注意到 $\widehat{D}_x$ 中不可能有最大元, 从而 $\hat{F}\setminus\widehat{D}_x$ 中有最小元. 记 $\widehat{C}_x=\hat{F}\setminus\widehat{D}_x$, 且用 $\hat{x}$ 表示 $\widehat{C}_x$ 中最小元. 据此, 我们可规定 K 到 $\hat{F}$ 的如下映射:

$$\phi\colon x\longmapsto\hat{x}=\min(\widehat{C}_x),\quad x\in K.$$

由 $\hat{x}$ 的规定, 可知这样一个事实: 对于 $a\in F$ 以及 $x\in K$, $a<_{\hat{P}}\hat{x}$ (或 $\hat{x}<_{\hat{P}}a$) 当且仅当 $a<_Q x$ (或 $x<_Q a$).

现设 $x,y\in K$. 假若 $\hat{x}+\hat{y}<_{\hat{P}}\widehat{x+y}$, 则由 F 在 $\hat{F}$ 中的稠密性知, 有 $a\in F$, 使得 $\hat{x}+\hat{y}<_{\hat{P}}a<_{\hat{P}}\widehat{x+y}$. 由上面事实知, $a<_Q x+y$. 此外, 有 $b\in F$, 使得 $\hat{x}<_{\hat{P}}b<_{\hat{P}}a-\hat{y}$. 由上面事实又有, $x<_Q b$ 且 $y<_Q a-b$. 从而 $x+y<_Q a$, 矛盾. 因而 $\hat{x}+\hat{y}\geqslant_{\hat{P}}\widehat{x+y}$. 同理, $\hat{x}+\hat{y}\leqslant_{\hat{P}}\widehat{x+y}$. 于是 $\hat{x}+\hat{y}=\widehat{x+y}$, 即 $\phi(x+y)=\phi(x)+\phi(y)$.

为证明 $\phi(xy)=\phi(x)\phi(y)$, 我们先证明: $\phi(-x)=-\phi(x)$, 即 $\widehat{-x}=-\hat{x}$. 事实上, 如若 $-\hat{x}<_{\hat{P}}\widehat{-x}$, 则有 $a\in F$, 使得 $-\hat{x}<_{\hat{P}}a<_{\hat{P}}\widehat{-x}$. 由此有 $a<_Q -x$, 但 $-a<_Q x$, 矛盾. 从而 $-\hat{x}\geqslant_{\hat{P}}\widehat{-x}$. 同理, $-\hat{x}\leqslant_{\hat{P}}\widehat{-x}$. 于是有 $-\hat{x}=\widehat{-x}$, 即 $\phi(-x)=-\phi(x)$. 特别地, 可推出 $\phi(0)=0$. 下面证明 $\phi(xy)=\phi(x)\phi(y)$. 当 $x=0$ 时, 等式显然成立. 当 $x>_Q 0$ 时, $\hat{x}>_{\hat{P}}0$. 假若 $\widehat{xy}<_{\hat{P}}\hat{x}\hat{y}$, 则由 F 在 $\hat{F}$ 中的稠密性知, 有 $a\in F$, 使得 $\widehat{xy}<_{\hat{P}}a<_{\hat{P}}\hat{x}\hat{y}$. 从而有 $xy<_Q a$, 且 $a\hat{x}^{-1}<_{\hat{P}}\hat{y}$. 又由 F 在 $\hat{F}$ 中的稠密性知, 有非零 $b\in F$, 使得 $a\hat{x}^{-1}<_{\hat{P}}b<_{\hat{P}}\hat{y}$. 由此有 $b<_Q y$, 且 $ab^{-1}<_Q x$. 于是 $a<_Q xy$, 矛盾. 从而 $\widehat{xy}\geqslant_{\hat{P}}\hat{x}\hat{y}$. 同理, $\widehat{xy}\leqslant_{\hat{P}}\hat{x}\hat{y}$. 因而 $\widehat{xy}=\hat{x}\hat{y}$. 当 $x<_Q 0$

即 $-x >_Q 0$ 时，$\widehat{xy} = -\widehat{(-x)y} = -(\widehat{-x})\hat{y} = -(-\hat{x})\hat{y} = \hat{x}\hat{y}$. 这表明：对于 $x, y \in K$, 总有 $\phi(xy) = \phi(x)\phi(y)$.

因而，映射 ϕ 是一个环同态. 注意到 K 是一个域，从而 ϕ 是一个嵌入. 易知，对于每个 $a \in F$, $\hat{a} = a$. 于是，ϕ 是一个 F- 嵌入. 设 $x <_Q y$, 其中 $x, y \in K$. 由 F 在 K 中的稠密性知，有 $a \in F$, 使得 $x <_Q a <_Q y$. 由此有 $\hat{x} <_{\hat{P}} a <_{\hat{P}} \hat{y}$, 即 $\phi(x) <_{\hat{P}} \phi(y)$. 这表明 ϕ 是保序的.

同样，存在序域 $(\hat{F}, \hat{P})$ 到 (K, Q) 的一个保序 F- 嵌入 ψ. 假若对于某个 $z \in \hat{F}$, $\phi \circ \psi(z) \neq z$, 则有 $\phi \circ \psi(z) <_{\hat{P}} z$ 或 $\phi \circ \psi(z) >_{\hat{P}} z$. 不妨设 $\phi \circ \psi(z) <_{\hat{P}} z$. 由 F 在 $\hat{F}$ 中的稠密性知，有 $a \in F$, 使得 $\phi \circ \psi(z) <_{\hat{P}} a <_{\hat{P}} z$. 此时，$\phi(\psi(z)) <_{\hat{P}} a = \phi(\psi(a))$. 由 ϕ 和 ψ 的保序性可知，$z <_{\hat{P}} a$, 矛盾. 因而，$\phi \circ \psi$ 是 $\hat{F}$ 上一个恒等映射. 自然，ϕ 是一个满射. 因此 ϕ 是一个保序 F- 同构. 证毕.

实际上，由上面证明可见，所求的保序 F- 同构 ϕ 是惟一的.

定理 6.9.6 设 (K, Q) 是一个序域，R 是它的实闭包，F 是 K 的子域，使得对于由 Q 所确定的区间拓扑，F 在 K 中稠密，则 F 在 R 中的代数闭包在 R 中稠密.

证明 由于 F 在 K 中稠密，从而 Q 显然在 F 上是阿基米德的. 又由定理 1.4.2 知，R 的惟一正锥 R^2 在 K 上也是阿基米德的. 于是，R^2 在 F 上是阿基米德的. 设 R_F 是 F 在 R 中的代数闭包，且记 $P = Q \cap F$.

设 $\alpha, \beta \in R$, 其中 $\alpha <_{R^2} \beta$. 由于 R^2 在 F 上是阿基米德的，从而有正元素 $c \in P$, 使得 $\frac{1}{2}(\beta - \alpha) >_{R^2} c$. 令 $\frac{1}{2}(\alpha + \beta)$ 在 K 上的极小多项式为 $f(x) = x^n + \beta_1 x^{n-1} + \cdots + \beta_n$, 其中 $\beta_i \in K$, $i = 1, \cdots, n$. 由引理 4.2.3 的推论知，有正元素 $d \in P$, 使得只要 $R[x]$ 中多项式 $g(x) = x^n + b_1 x^{n-1} + \cdots + b_n$ 满足 $|\beta_i - b_i|_{R^2} <_{R^2} d$, $i = 1, \cdots, n$, 多项式 $g(x)$ 在 R 中必有一个根 y, 且满足 $|\frac{1}{2}(\alpha + \beta) - y|_{R^2} <_{R^2} c$. 由于 F 在 K 中稠密，从而有 $b_i \in F$, 使得 $|\beta_i - b_i|_Q <_Q d$, 即 $|\beta_i - b_i|_{R^2} <_{R^2} d$, $i = 1, \cdots, n$. 此时，$g(x) = x^n + b_1 x^{n-1} + \cdots + b_n \in F[x]$, 且 $g(x)$ 在 R 中有一个根 y_1, 使得 $|\frac{1}{2}(\alpha + \beta) - y_1|_{R^2} <_{R^2} c$. 显然，$y_1 \in R_F$, 且 $\alpha = \frac{\alpha + \beta}{2} + \frac{\alpha - \beta}{2} <_{R^2} \frac{\alpha + \beta}{2} - c <_{R^2} \frac{\alpha + \beta}{2} + \left(y_1 - \frac{\alpha + \beta}{2}\right) = y_1$, 而 $\beta = \frac{\alpha + \beta}{2} - \frac{\alpha - \beta}{2} >_{R^2} \frac{\alpha + \beta}{2} + c >_{R^2} \frac{\alpha + \beta}{2} + \left(y_1 - \frac{\alpha + \beta}{2}\right) = y_1$. 因此，$R_F$ 在 R 中稠密. 证毕.

推论 1 设 $(\hat{F}, \hat{P})$ 是序域 (F, P) 的完全化，则 $\hat{F}$ 是实闭域，当且仅当 F 在它关于 P 的实闭包中稠密.

证明 设 $\hat{F}$ 是实闭域，且令 R_F 是 F 在 $\hat{F}$ 中的代数闭包. 由命题 2.1.5 知，R_F 是序域 (F, P) 的实闭包. 由于 F 在 $\hat{F}$ 中稠密，从而 F 显然在 R_F 中稠密.

反过来，设 F 在它关于 P 的实闭包中稠密. 令 R 是 $(\hat{F}, \hat{P})$ 的实闭包，且 R_F

是 F 在 R 中的代数闭包. 由定理 6.9.6 知, R_F 在 R 中稠密. 由命题 2.1.5 知, R_F 是 (F,P) 的实闭包. 由所设, F 在 R_F 中稠密. 由此知, F 在 R 中稠密. 此时, 显然 $\hat{F}$ 在 R 中稠密. 由 $(\hat{F},\hat{P})$ 的完全性有, $\hat{F}=R$, 即 $\hat{F}$ 是实闭域. 证毕.

推论 2 极大序域的完全化还是一个极大序域.

第七章　Tarski-Seidenberg 原理与转移定理

在本章中，我们将建立著名的 Tarski-Seidenberg 原理．在此基础上，一个适合实闭域的重要定理 —— 转移定理被建立．作为转移定理的应用，我们证明了一些重要定理，例如实零点定理等．

§7.1　模型论中有关概念

为了后面讨论的需要，本节将介绍模型论中一些基本概念和结论．

域的初等语言简称作域语言，它是由如下符号组成：

(1) 个体符号：$0, 1, x_1, \cdots, x_n, \cdots$，其中 0 和 1 称作个体常量，$x_1, \cdots, x_n, \cdots$，称作个体变量；

(2) 运算符号：$+, -, \cdot$；

(3) 关系符号：$=$；

(4) 逻辑关联词：$\sim, \wedge, \vee, \forall, \exists$；

(5) 括号：(,)．

域语言的一个结构是如下一个六要素组合：

$$\mathcal{A} = (A, +^{\mathcal{A}}, -^{\mathcal{A}}, \cdot^{\mathcal{A}}, 0^{\mathcal{A}}, 1^{\mathcal{A}}),$$

其中 A 是一个非空集合，$0^{\mathcal{A}}$, $1^{\mathcal{A}} \in A$, $+^{\mathcal{A}}$: $A \times A \longrightarrow A$, $-^{\mathcal{A}}: A \longrightarrow A$, $\cdot^{\mathcal{A}}$: $A \times A \longrightarrow A$ 是集合 A 上的 (一元和二元) 运算．此时，$+^{\mathcal{A}}, -^{\mathcal{A}}, \cdot^{\mathcal{A}}, 0^{\mathcal{A}}$ 和 $1^{\mathcal{A}}$ 分别称作符号 $+, -, \cdot, 0$ 和 1 在 $\mathcal{A}$ 中的解释．在下面，结构 $\mathcal{A}$ 中第一要素 A 常用 $|\mathcal{A}|$ 表示．

若在域语言中增加一个新的关系符号 $<$，则构成的语言称作序域的初等语言，或简称序域语言．序域语言的一个结构是如下一个七要素组合：

$$\mathcal{A} = (A, +^{\mathcal{A}}, -^{\mathcal{A}}, \cdot^{\mathcal{A}}, 0^{\mathcal{A}}, 1^{\mathcal{A}}, <^{\mathcal{A}}),$$

其中前面六要素组合 $(A, +^{\mathcal{A}}, -^{\mathcal{A}}, \cdot^{\mathcal{A}}, 0^{\mathcal{A}}, 1^{\mathcal{A}})$ 是域语言的一个结构，$<^{\mathcal{A}}$ 是集 A 上一个二元关系．此时，$<^{\mathcal{A}}$ 称作符号 $<$ 在 $\mathcal{A}$ 中的解释．

有时，需要在域语言或序域语言中增补有限个新的个体常量符号：$c_1, \cdots, c_n$，由此得到扩充的相应语言．此时，扩充的语言的一个结构是这样一个组合 $\mathcal{B} = (\mathcal{A}, a_1, \cdots, a_n)$，其中 $\mathcal{A}$ 为原来语言的一个结构，且 $a_1, \cdots, a_n \in |\mathcal{A}|$．很自然，$a_1, \cdots, a_n$ 依次称作所增补的个体常量符号 $c_1, \cdots, c_n$ 在 $\mathcal{B}$ 中的解释，且记作 $c_i^{\mathcal{A}} = a_i$，$i = 1, \cdots, n$．

对于增补常量符号 $c_1, \cdots, c_n$ 所得到的扩充的域语言，我们可按如下方式递归地定义项集 Tm_n:

(i)$0, 1, c_1, \cdots, c_n, x_1, x_2, \cdots \in \mathrm{Tm}_n$;

(ii) 若 $t_1, t_2 \in \mathrm{Tm}_n$, 则 $t_1 + t_2, t_1 \cdot t_2, -t_1 \in \mathrm{Tm}_n$.

当 $n = 0$ 时， Tm_n 为原来域语言的项集．项集 Tm_n 中一个表达式称作扩充的域语言中一个项．

同时，公式集 Fml_n 可递归地定义如下：

(1) 对于所有 $t_1, t_2 \in \mathrm{Tm}_n$, $t_1 = t_2 \in \mathrm{Fml}_n$;

(2) 若 $\phi, \psi \in \mathrm{Fml}_n$, 则 $\sim \phi, \phi\wedge\psi, \phi\vee\psi, \forall x\phi, \exists x\phi \in \mathrm{Fml}_n$, 其中 $x \in \{x_1, x_2, \cdots\}$.

公式集 Fml_n 中一个表达式称作扩充的域语言中一个公式． 如 (1) 所定义的公式 $t_1 = t_2$ 称作原始公式.

对于扩充的序域语言，规定它的项集 $\mathrm{Tm}_n^<$ 与域语言的项集相同，即 $\mathrm{Tm}_n^< = \mathrm{Tm}_n$. 而它的公式集 Fml_n 被递归地定义如下：

(1′) 对于所有 $t_1, t_2 \in \mathrm{Tm}_n^<$, $t_1 = t_2$, $t_1 < t_2 \in \mathrm{Fml}_n^<$;

(2′) 同上面的规定 (2).

同样，按 (1′) 所规定的公式称作序域语言中原始公式. 为简明起见，我们约定：公式 $\sim (t_1 = t_2)$ 简记作 $t_1 \neq t_2$; $t_1 = t_2 \vee t_1 < t_2$ 简记作 $t_1 \leqslant t_2$; $(\sim \phi) \vee \psi$ 简记作 $\phi \longrightarrow \psi$; $(\phi \longrightarrow \psi) \wedge (\psi \longrightarrow \phi)$ 简记作 $\phi \longleftrightarrow \psi$, 而 $\forall x_1 \cdots \forall x_n\phi$ $(\exists x_1 \cdots \exists x_n\phi)$ 简记作 $\forall(x_1, ..., x_n)\phi$ $(\exists(x_1, ..., x_n)\phi)$.

用 Vbl 表示由个体变量符号组成的集合，即 $\mathrm{Vbl} = \{x_1, x_2, \cdots\}$. 一个项 $t \in \mathrm{Tm}_n$ 称作常量项， 如果 t 中不出现 Vbl 中变量. 借助于归纳原理，对于一个结构 $\mathcal{A}$, 常量 t 在 $\mathcal{A}$ 中的解释 $t^{\mathcal{A}}$ 可通过 $0^{\mathcal{A}}, 1^{\mathcal{A}}, c_1^{\mathcal{A}}, \cdots, c_n^{\mathcal{A}}$ 规定如下：

当t的形式为$t_1 + t_2$, $-t_1$或$t_1 \cdot t_2$时, $t^{\mathcal{A}} = t_1^{\mathcal{A}} +^{\mathcal{A}} t_2^{\mathcal{A}}$, $-^{\mathcal{A}} t_1^{\mathcal{A}}$或$t_1^{\mathcal{A}} \cdot^{\mathcal{A}} t_2^{\mathcal{A}}$.

因此，对于每个常量项 t, $t^{\mathcal{A}} \in |\mathcal{A}|$. 换言之， $t \longmapsto t^{\mathcal{A}}$ 是 Tm_n 中所有常量项到 $|\mathcal{A}|$ 的一个映射.

对于 Fml_n 或 $\mathrm{Fml}_n^<$ 中一个公式 ϕ, 可定义 ϕ 的自由变量集 $\mathrm{Fr}(\phi)$ 如下：

$$\mathrm{Fr}(t_1 = t_2) = \mathrm{Fr}(t_1 < t_2) = \{x \in \mathrm{Vbl} \mid x\text{出现在}t_1\text{或}t_2\text{中}\};$$
$$\mathrm{Fr}(\sim \psi) = \mathrm{Fr}(\psi);$$
$$\mathrm{Fr}(\psi_1 \wedge \psi_2) = \mathrm{Fr}(\psi_1 \vee \psi_2) = \mathrm{Fr}(\psi_1) \cup \mathrm{Fr}(\psi_2);$$
$$\mathrm{Fr}(\forall x\psi) = \mathrm{Fr}(\exists x\psi) = \mathrm{Fr}(\psi) \setminus \{x\}.$$

集合 $\mathrm{Fr}(\phi)$ 中元素称作公式 ϕ 的自由变量．没有自由变量的公式称作语句．用 Sent_n 和 $\mathrm{Sent}_n^<$ 分别表示公式集 Fml_n 和 $\mathrm{Fml}_n^<$ 中全部语句组成的集合. 显然，$\mathrm{Sent}_n \subseteq \mathrm{Sent}_n^<$.

设 $\phi \in \mathrm{Sent}_n^<$, 且 $\mathcal{B} = (\mathcal{A}, a_1, \cdots, a_n)$ 是扩充的序域语言的一个结构，则我们可以递归地定义关系式 $\mathcal{B} \models \phi$ 如下：

$\mathcal{B} \models t_1 = t_2$当且仅当$t_1^{\mathcal{B}} = t_2^{\mathcal{B}}$;
$\mathcal{B} \models t_1 < t_2$当且仅当$t_1^{\mathcal{B}} <^{\mathcal{B}} t_2^{\mathcal{B}}$;
$\mathcal{B} \models \sim \psi$当且仅当$\mathcal{B} \models \psi$被否定;
$\mathcal{B} \models \psi_1 \wedge \psi_2$当且仅当$\mathcal{B} \models \psi_1$且$\mathcal{B} \models \psi_2$;
$\mathcal{B} \models \psi_1 \vee \psi_2$当且仅当$\mathcal{B} \models \psi_1$或$\mathcal{B} \models \psi_2$;
$\mathcal{B} \models \forall x\psi$当且仅当对于每个$a \in |\mathcal{A}|, (\mathcal{B}, a) \models \psi(c_{n+1})$;
$\mathcal{B} \models \exists x\psi$当且仅当对于某个$a \in |\mathcal{A}|, (\mathcal{B}, a) \models \psi(c_{n+1})$.

在上面表达中, $\psi(c_{n+1})$ 表示用新常量符号 c_{n+1} 代换公式 ψ 中作为自由变量而出现的所有 x 而得到的语句, 例如, 当 ψ 为 $\exists x(x^2 = 1) \wedge x < 0$ 时, $\psi(c_{n+1})$ 为语句 $\exists x(x^2 = 1) \wedge c_{n+1} < 0$. 这样, 对于每个 $\phi \in \mathrm{Sent}_n^{<}$ 以及扩充的序域语言的一个结构 $\mathcal{B}$, 要么有 $\mathcal{B} \models \phi$, 要么 $\mathcal{B} \models \phi$ 被否定.

用 C_n 和 $C_n^{<}$ 分别表示扩充的域语言和序域语言中全部结构组成的类. 为统一讨论起见, 用 C 代表 C_n 和 $C_n^{<}$ 中任意一个类, 且用 Sent 表示相应语言的语句集.

对于 Sent 的一个子集 Σ, C 中一个结构 $\mathcal{A}$ 称作 Σ 的一个模型, 如果对于每个 $\phi \in \sum$, $\mathcal{A} \models \phi$. $\sum$ 的所有模型构成的类称作 $\sum$ 的模型类, 且记作 $\mathrm{mod}(\sum)$. C 的一个子类 E 称作一个模型类 (或初等类), 如果 E 是 Sent 的某个子集 $\sum$ 的模型类. 此时亦称: E 是可公理化的, 且 $\sum$ 称作 E 的一个公理系. 特别地, 若 E 是 Sent 的某个有限子集的模型类, 则称 E 是有限可公理化的.

例 1 考察 C_0 的如下子类:

(1) 所有域组成的类是初等类, 且该类是有限可公理化的.

构造由如下语句组成的子集 Σ_F:

$$
\begin{aligned}
&\forall x_1 \forall x_2 (x_1 + x_2 = x_2 + x_1),\\
&\forall x_1 \forall x_2 \forall x_3 \big((x_1 + x_2) + x_3 = x_1 + (x_2 + x_3)\big),\\
&\forall x_1 \big(x_1 + 0 = x_1 \wedge x_1 + (-x_1) = 0\big),\\
&\forall x_1 \forall x_2 (x_1 \cdot x_2 = x_2 \cdot x_1),\\
&\forall x_1 (x_1 \cdot 1 = x_1),\\
&\forall x_1 \forall x_2 \forall x_3 \big((x_1 \cdot x_2) \cdot x_3 = x_1 \cdot (x_2 \cdot x_3)\big),\\
&\forall x_1 \forall x_2 \forall x_3 \big((x_1 + x_2) \cdot x_3 = (x_1 \cdot x_3) + (x_2 \cdot x_3)\big),\\
&\forall x_1 \big(x_1 = 0 \vee \exists x_2 (x_1 \cdot x_2 = 1)\big).
\end{aligned}
$$

由域的定义知, $\mathrm{mod}(\Sigma_F)$ 即为所有域组成的类.

(2) 所有实域组成的类是初等类. 对于每个自然数 n, 用 ϕ_n 表示如下语句:

$$\forall (x_1 \cdots x_n)(x_1^2 + \cdots + x_n^2 \neq -1).$$

于是，所有实域组成 $\Sigma_F \cup \{\phi_n \mid n = 1, 2, \cdots\}$ 的模型类.

(3) 所有实闭域组成的类是初等类. 对于每个自然数 n, 用 Ψ_n 表示如下语句：

$$\forall(x_1 \cdots x_{2n-1})\exists x_{2n}(x_{2n}^{2n-1} + x_{2n-1}x_{2n}^{2n-2} + \cdots + x_1 = 0).$$

由定理 2.1.3 知，实闭域类的一个公理系由 $\Sigma_F \cup \{\Psi_n \mid n = 1, 2, \cdots\}$ 中全部语句以及如下三个语句所组成：

$$\forall x_1 \forall x_2 \exists x_3 (x_1^2 + x_2^2 = x_3^2),$$
$$\forall x_1 (x_1^2 \neq -1),$$
$$\forall x_1 \exists x_2 \big((x_1 = x_2^2) \vee (-x_1 = x_2^2)\big).$$

例 2 考虑 $C_0^<$ 的如下子类：

(1) 所有序域组成的类是初等类，它的一个公理系可通过在域类的公理系 Σ_F 上再添加下面语句而得到：

$$\forall x_1 \forall x_2 \forall x_3 (x_1 \leqslant x_2 \wedge x_2 \leqslant x_3 \longrightarrow x_1 \leqslant x_3),$$
$$\forall x_1 \forall x_2 (x_1 \leqslant x_2 \wedge x_2 \leqslant x_1 \longrightarrow x_1 = x_2),$$
$$\forall x_1 \forall x_2 (x_1 \leqslant x_2 \vee x_2 \leqslant x_1),$$
$$\forall x_1 \forall x_2 \big(x_1 \leqslant x_2 \longrightarrow \forall x_3 (x_1 + x_3 \leqslant x_2 + x_3)\big),$$
$$\forall x_1 \forall x_2 (0 \leqslant x_1 \wedge 0 \leqslant x_2 \longrightarrow 0 \leqslant x_1 x_2).$$

(2) 所有极大序域组成的类是初等类. 为得到它的一个公理系，只须在序域类的如上公理系上再添加例 1 (3) 中全部语句 Ψ_n, $n = 1, 2, \cdots$, 以及这样一个语句：

$$\forall x_1 \big(0 < x_1 \longrightarrow \exists x_2 (x_1 = x_2^2)\big).$$

例 3 考虑 C_{n+1} 和 $C_{n+1}^<$ 的如下子类：

(1) 设 ψ 为如下语句：

$$\exists x_1 (c_{n+1} x_1^n + c_n x_1^{n-1} + \cdots + c_1 = 0),$$

且 Σ_F 是例 1(1) 中所示的域类的公理系，则模型类 $\mathrm{mod}(\Sigma_F \cup \{\psi\})$ 是由 C_{n+1} 中所有这样的结构 $(\mathcal{A}, a_1, \cdots, a_{n+1})$ 所组成的，其中 $\mathcal{A}$ 是域类中一个结构， $a_1, \cdots, a_{n+1} \in |\mathcal{A}|$, 使得多项式 $a_{n+1}x^n + a_n x^{n-1} + \cdots + a_1$ 在 $|\mathcal{A}|$ 中有根.

(2) 设 ϕ 为如下语句：

$$\exists x_1 (c_{n+1} x_1^n + c_n x_1^{n-1} + \cdots + c_1 > 0),$$

且 Σ_O 是例 2(1) 中所示的序域类的公理系，则模型类 $\mathrm{mod}(\Sigma_O \cup \{\phi\})$ 是由 $C_{n+1}^<$ 中所有这样的结构 $(\mathcal{A}, a_1, \cdots, a_{n+1})$ 所组成的，其中 $\mathcal{A}$ 是序域类中一个结构，$a_1, \cdots, a_{n+1} \in |\mathcal{A}|$, 使得多项式 $a_{n+1}x^n + a_n x^{n-1} + \cdots + a_1$ 在 $|\mathcal{A}|$ 上有正值.

现设 Γ 是 Sent 的一个子集，且 Γ 关于 $\wedge, \vee$ 和 $\sim$ 是闭的，即对于 $\phi, \psi \in \Gamma$, 总

有 $\phi\wedge\psi$, $\phi\vee\psi$, $\sim\phi\in\Gamma$. C 中两个结构 $\mathcal{A}$ 和 $\mathcal{B}$ 称作 Γ- 等价，如果对于每个 $\gamma\in\Gamma$, $\mathcal{A}\models\gamma$ 当且仅当 $\mathcal{B}\models\gamma$. 此时，记作： $\mathcal{A}\equiv_\Gamma\mathcal{B}$. 特别地，当 $\Gamma=$Sent 时，称 $\mathcal{A}$ 和 $\mathcal{B}$ 是初等等价的，且记作： $\mathcal{A}\equiv\mathcal{B}$.

一类重要的语句是所谓的无量词语句. 一个语句 γ 称作是无量词的，如果 γ 中没有量词符号 $\forall$ 和 $\exists$ 出现. 用 Γ_n 和 $\Gamma_n^{\leqslant}$ 分别表示由 Sent_n 和 $\mathrm{Sent}_n^{\leqslant}$ 中所有无量词语句组成的子集. 显然， Γ_n 和 $\Gamma_n^{\leqslant}$ 关于 $\wedge,\vee$ 和 $\sim$ 都是闭的.

定义 7.1.1　C_0 (或 $C_0^{\leqslant}$) 的一个子类 E 被称作容许量词消去， 如果对于每个 $\psi\in\mathrm{Sent}_n$ (或 $\mathrm{Sent}_n^{\leqslant}$), 总有 $\gamma\in\Gamma_n$ (或 $\Gamma_n^{\leqslant}$), 使得对于 E 中每个结构 $\mathcal{A}$ 以及任意 $a_1,\cdots,a_n\in|\mathcal{A}|$, $(\mathcal{A},a_1,\cdots,a_n)\models(\psi\longleftrightarrow\gamma)$. 此时，称 ψ 模 E 等价于 γ.

设 $\mathcal{A}$ 和 $\mathcal{B}$ 是 C_0 (或 $C_0^{\leqslant}$) 中两个结构. 称 $\mathcal{A}$ 是 $\mathcal{B}$ 的一个子结构，如果 $|\mathcal{A}|\subseteq|\mathcal{B}|$, $0^{\mathcal{A}}=0^{\mathcal{B}}$, $1^{\mathcal{A}}=1^{\mathcal{B}}$, 且 $|\mathcal{A}|$ 上的运算 $+^{\mathcal{A}}$, $-^{\mathcal{A}}$, $\cdot^{\mathcal{A}}$ (以及关系 $<^{\mathcal{A}}$) 分别是 $+^{\mathcal{B}}$, $-^{\mathcal{B}}$, $\cdot^{\mathcal{B}}$(以及 $<^{\mathcal{B}}$) 在 $|\mathcal{A}|$ 上的限制. 此时，记作 $\mathcal{A}\subseteq\mathcal{B}$. 我们称 $\mathcal{A}$ 是 $\mathcal{B}$ 的一个初等子结构，如果 $\mathcal{A}\subseteq\mathcal{B}$, 且对于任意有限个 $a_1,\cdots,a_n\in|\mathcal{A}|$, $(\mathcal{A},a_1,\cdots,a_n)\equiv(\mathcal{B},a_1,\cdots,a_n)$. 此时，记作 $\mathcal{A}\preceq\mathcal{B}$.

容许量词消去的结构类具有如下重要性质.

命题 7.1.1　设 E 是 C_0 (或 $C_0^{\leqslant}$) 的一个容许量词消去的子类，则对于 $\mathcal{A},\mathcal{B}\in E$, 由 $\mathcal{A}\subseteq\mathcal{B}$ 可推出 $\mathcal{A}\preceq\mathcal{B}$.

证明　设 $\psi\in\mathrm{Sent}_n$ (或 $\mathrm{Sent}_n^{\leqslant}$), 其中 n 为任意自然数. 由所设知，有 $\gamma\in\Gamma_n$ (或 $\Gamma_n^{\leqslant}$), 使得 ψ 模 E 等价于 γ. 从而对于任意 $a_1,\cdots,a_n\in|\mathcal{A}|\subseteq|\mathcal{B}|$,

$$(\mathcal{A},a_1,\cdots,a_n)\models(\psi\longleftrightarrow\gamma),$$

并且

$$(\mathcal{B},a_1,\cdots,a_n)\models(\psi\longleftrightarrow\gamma).$$

由于 γ 中无量词，从而显然有 $(\mathcal{A},a_1,\cdots,a_n)\models\gamma$ 当且仅当 $(\mathcal{B},a_1,\cdots,a_n)\models\gamma$. 由此可得

$$(\mathcal{A},a_1,\cdots,a_n)\models\psi \text{ 当且仅当 } (\mathcal{B},a_1,\cdots,a_n)\models\psi.$$

这表明 $(\mathcal{A},a_1,\cdots,a_n)\equiv(\mathcal{B},a_1,\cdots,a_n)$. 因此， $\mathcal{A}\preceq\mathcal{B}$. 证毕.

§7.2　Tarski-Seidenberg 原理

著名的 Tarski-Seidenberg 原理是由 A. Tarski 首先提出的. 随后，A. Seidenberg 对这一原理给出了新的处理方法. 在本节中，我们将采用更新的方式来建立 Tarski-Seidenberg 原理.

设 R 是一个实闭域，且 $\leqslant$ 是 R 的惟一序. 对于 $a\in R$, 用 $\mathrm{sgn}(a)$ 表示 a 关于

序 $\leqslant$ 的符号，即当 $a=0$, $a>0$ 或 $a<0$ 时，分别规定 $\operatorname{sgn}(a)=0$, $\operatorname{sgn}(a)=1$ 或 $\operatorname{sgn}(a)=-1$.

对于一元多项式环 $R[x]$ 中一组不全为零的多项式 $f_1,\cdots,f_s$, 设 $\alpha_1<\alpha_2<\cdots<\alpha_N$ 是该组中所有非零多项式在 R 中的全部根. 约定 $\alpha_0=-\infty$, 且 $\alpha_{N+1}=+\infty$. 同时, 记 $I_k=]\alpha_k,\alpha_{k+1}[$ 是 R 中端点为 α_k 和 α_{k+1} 的开区间，$k=0,1,\cdots,N$. 由中间值定理知，当 x 在 I_k 中取值时，$\operatorname{sgn}(f_i(x))$ 保持不变，因而用 $\operatorname{sgn}(f_i(I_k))$ 来表示这一固定不变的符号，$i=1,\cdots,s$; $k=0,1,\cdots,N$.

据此，我们可以得到一个表值在 $\{-1,1,0\}$ 中的 $s\times(2N+1)$ 矩阵，其中第 i 行为

$$\operatorname{sgn}\big(f_i(I_0)\big), \operatorname{sgn}\big(f_i(\alpha_1)\big), \operatorname{sgn}\big(f_i(I_1)\big), \cdots, \operatorname{sgn}\big(f_i(\alpha_N)\big), \operatorname{sgn}\big(f_i(I_N)\big).$$

这样一个矩阵记作 $\mathrm{SGN}_R(f_1,\cdots,f_s)$.

显然，矩阵 $\mathrm{SGN}_R(f_1,\cdots,f_s)$ 具有这样的特性：(1) 若 f_i 为非零多项式，则在该矩阵的第 i 行中，列指标为奇数的表值不为零，且任意两个相邻的非零表值相同 (都为 -1 或都为 1); (2) 任意相邻的两列不是完全相同的.

令 $m=\max\{\deg f_i \mid i=1,\cdots,s\}$, 则 $N\leqslant sm$. 用 $W_{s,m}$ 表示所有表值在 $\{-1,0,1\}$ 中的 $s\times(2t+1)$ 矩阵组成的集合，其中 t 取遍 $0,1,\cdots,sm$.

引理 7.2.1 所设同上，且 ϵ 是集 $\{1,\cdots,s\}$ 到 $\{-1,0,1\}$ 的一个映射，则存在 $W_{s,m}$ 的一个子集 $W(\epsilon)$, 使得对于任意一个实闭域 R 以及 $R[x]$ 中任意 s 个次数不超过 m 的多项式 $f_1,\cdots,f_s$, 关系式组

$$\begin{cases} \operatorname{sgn}\big(f_1(x)\big) &= \epsilon(1) \\ \operatorname{sgn}\big(f_2(x)\big) &= \epsilon(2) \\ \qquad\cdots\cdots & \\ \operatorname{sgn}\big(f_s(x)\big) &= \epsilon(s) \end{cases}$$

在 R 中有解，当且仅当 $\mathrm{SGN}_R(f_1,\cdots,f_s)\in W(\epsilon)$.

证明 设 $W(\epsilon)$ 是由 $W_{s,m}$ 中所有这样的矩阵组成的集合，这些矩阵中有一列元素自上而下依次为：$\epsilon(1),\cdots,\epsilon(s)$. 显然，$W(\epsilon)$ 为所求. 证毕.

引理 7.2.2 设 R 是一个实闭域，$f_1,\cdots,f_s\in R[x]$ 是一组不全为零的多项式，且它们在 R 中的全部根为 $\alpha_1<\alpha_2<\cdots<\alpha_N$. 若 $\beta\in R$, 使得对于某个 $k\in\{1,\cdots,N-1\}$, $\alpha_k<\beta<\alpha_{k+1}$, 且 A 是这样一个 $s\times(2N+3)$ 矩阵，它的第 $i(i=1,\cdots,s)$ 行表值依次为

$$\operatorname{sgn}\big(f_i(]-\infty,\alpha_1[)\big), \operatorname{sgn}\big(f_i(\alpha_1)\big), \operatorname{sgn}\big(f_i(]\alpha_1,\alpha_2[)\big), \cdots, \operatorname{sgn}\big(f_i(]\alpha_k,\beta[)\big), \operatorname{sgn}\big(f_i(\beta)\big),$$
$$\operatorname{sgn}\big(f_i(]\beta,\alpha_{k+1}[)\big), \operatorname{sgn}\big(f_i(\alpha_{k+1})\big), \cdots, \operatorname{sgn}\big(f_i(\alpha_N)\big), \operatorname{sgn}\big(f_i(]\alpha_N,+\infty[)\big),$$

则矩阵 A 的第 $2k+1$, 第 $2k+2$ 和第 $2k+3$ 列完全相同，且在划去其中两列后，

即得矩阵 $\mathrm{SGN}_R(f_1,\cdots,f_s)$.

证明 注意到, 每个多项式 f_i 在开区间 $]\alpha_k,\alpha_{k+1}[$ 中保持符号不变. 从而 $\mathrm{sgn}(f_i(]$
α_k. $\mathrm{sgn}(f_i(\beta))=\mathrm{sgn}(f_i(]\beta,\alpha_{k+1}[))$, $i=1,\cdots,s$.

设 $\beta_1<\beta_2<\cdots<\beta_N$ 是 R 中元素序列, 使得 $f_1,\cdots,f_s$ 的全部根都在该序列中. 记 $I_0=]-\infty,\beta_1[$, $I_N=]\beta_N,+\infty[$, $I_k=]\beta_k,\beta_{k+1}[$, $k=1,\cdots,N-1$, 且 A 是这样一个 $s\times(2N+1)$ 矩阵, 它的第 i 行为

$$\mathrm{sgn}(f_i(I_0)),\ \mathrm{sgn}(f_i(\beta_1)),\ \mathrm{sgn}(f_i(I_1)),\ \cdots,\ \mathrm{sgn}(f_i(\beta_N)),\ \mathrm{sgn}(f_i(I_N)),$$

其中 $i=1,\cdots,s$.

此时, A 中可能有相邻的两列完全相同. 若 A 有相邻的两列完全相同, 则划掉其中一列. 如此一直进行下去, 直到获得这样一个矩阵, 其中任意相邻的两列都不完全相同. 根据引理 7.2.2 可知, 最后所得的矩阵恰为 $\mathrm{SGN}_R(f_1,\cdots,f_s)$.

命题 7.2.3 存在 $W_{2s,m}$ 到 $W_{s,m}$ 的一个映射 π, 使得对于任意一个实闭域 R 以及 $R[x]$ 中任意 s 个次数不超过 m 的多项式 $f_1,\cdots,f_s$, 其中 $f_s\notin R$, 且 $f_1,\cdots,f_s$ 都不为零,

$$\pi(\mathrm{SGN}_R(f_1,\cdots,f_{s-1},f_s',g_1,\cdots,g_s))=\mathrm{SGN}_R(f_1,\cdots,f_s),$$

其中 f_s' 为 f_s 的微商, $g_1,\cdots,g_s$ 是在带余除法下分别用 $f_1,\cdots,f_{s-1},f_s'$ 除 f_s 所得的余式.

证明 为了构造满足条件的映射, 必须对 $W_{2s,m}$ 中每个矩阵, 给予 $W_{s,m}$ 中一个确定的对应矩阵.

任意取定 $D\in W_{s,m}$. 对于 $A\in W_{2s,m}$, 若 A 的前 s 行中某行里, 有列指标为奇数的零表值, 或者某两个相邻的非零表值不相同, 则规定 $\pi(A)=D$. 对于 $W_{2s,m}$ 中其他矩阵 A, 将 A 的前 s 行中所有零表值的列指标按大小排列, 则得一个由偶数组成的数列 $j_1<j_2<\cdots<j_M$.

若 $M=0$, 即 A 的前 s 行中根本没有零表值, 则 A 的前 s 行中每行的表值保持相同. 此时, 规定 $\pi(A)$ 是这样一个 $s\times 3$ 矩阵, 它的前 $s-1$ 行的表值与 A 的前 $s-1$ 行表值分别相等, 而第 s 行为 $(-1,0,1)$ 或 $(1,0,-1)$, 根据 A 的第 s 行的表值为 1 或 -1 而定.

现设 $M>0$. 对于 $k=1,\cdots,M$, 在 A 的前 s 行中, 必有某一行, 其中列指标为 j_k 的表值为零. 取定这样的行, 且用 $\theta(k)$ 表示该行的行指标. 显然, $1\leqslant\theta(k)\leqslant s$, $k=1,\cdots,M$.

设 A 是一个 $2s\times(2t+1)$ 矩阵, $1\leqslant t\leqslant 2sm$, 且用 $a_{i,j}$ 表示矩阵 A 中行指标为 i 且列指标为 j 的表值, $i=1,\cdots,2s$; $j=1,\cdots,2t+1$. 现根据下列情况, 对数列 $j_1<j_2<\cdots<j_M$ 进行处理:

(1) 对于每对数组 (j_k,j_{k+1}), $k=1,\cdots,M-1$, 若

$$a_{s+\theta(k),j_k}\cdot a_{s+\theta(k+1),j_{k+1}}=-1,$$

则在 j_k 和 j_{k+1} 之间插入奇数 j_k+1. 否则, j_k 和 j_{k+1} 之间不插入新数, 仍保持 j_k 和 j_{k+1} 的相邻关系.

(2) 若 $a_{s,1}\cdot a_{s+\theta(1),j_1}=-1$, 则在 j_1 之前添加奇数 j_1-1. 否则, 仍保持 j_1 在首位.

(3) 若 $a_{s,2t+1}\cdot a_{s+\theta(M),j_M}=-1$, 则在 j_M 之后添加奇数 j_M+1. 否则, 仍保持 j_M 在末位.

经过上面的处理后, 原来的数列 $j_1<j_2<\cdots<j_M$ 将因插入奇数而扩大为新的数列 $r_1<r_2<\cdots<r_N$, 其中 $M\leqslant N$.

现在, 可构造一个 $s\times(2N+1)$ 级矩阵 A_1, 使得下列条件成立:

(i) 对于 $i=1,\cdots,s-1$, 第 i 行元素依次为

$$a_{i,1},\ a_{i,r_1},\ a_{i,r_1'},\ a_{i,r_2},\ a_{i,r_2'},\ \cdots,\ a_{i,r_N},\ a_{i,2t+1},$$

其中 $r_e'=r_e$, 若 r_e 为奇数; 或者 $r_e'=r_e+1$, 若 r_e 为偶数, $e=1,\cdots,N$.

(ii) 第 s 行元素依次为

$$b_0,\ b_{r_1},\ b_{r_1'},\ b_{r_2},\ b_{r_2'},\ \cdots,\ b_{r_N},\ b_{r_N'},$$

其中

$$b_0=\begin{cases}-a_{s,1}, & 若 r_1 为奇数,\\ a_{s+\theta(k),j_k}, & 若 r_1=j_k\in\{j_1,\cdots,j_M\},\end{cases}$$

$$b_{r_e}=\begin{cases}0, & 若 r_e 为奇数,\\ a_{s+\theta(k),j_k}, & 若 r_e=j_k\in\{j_1,\cdots,j_M\},\end{cases}$$

$$b_{r_e'}=\begin{cases}a_{s,r_e+1}, & 若 r_e 为奇数,\\ a_{s+\theta(k),j_k}, & 若 r_e=j_k\in\{j_1,\cdots,j_M\},\end{cases}$$

这里 $e=1,\cdots,N$.

在矩阵 A_1 中, 若有相邻的两列完全相同, 则划去其中一列. 如此进行下去, 直到得到这样一个矩阵 A_2, 其中任意相邻的两列都不完全相同. 当 $A_2\in W_{s,m}$ 时, 规定 $\pi(A)=A_2$; 否则, 规定 $\pi(A)=D$.

这样, 对于 $W_{2s,m}$ 中每个矩阵, 在 $W_{s,m}$ 中都有一个确定的矩阵 $\pi(A)$ 与之对应. 换句话说, π 是 $W_{2s,m}$ 到 $W_{s,m}$ 的一个映射. 下面证明映射 π 满足引理中所要求的条件.

设 R 是任意实闭域, $f_1,\cdots,f_s$ 是 $R[x]$ 中次数不超过 m 的多项式, 其中 $f_s\notin R$, 且 $f_1,\cdots,f_{s-1}$ 都不为零, 同时 f_s' 以及 $g_1,\cdots,g_s$ 是如引理所示的多项式. 显然, $f_s'\neq 0$.

令 $A=\mathrm{SGN}_R(f_1,\cdots,f_{s-1},f_s',g_1,\cdots,g_s)$, 其中 $A=(a_{i,j})_{2s\times(2t+1)}\in W_{2s,m}$,

$1 \leqslant t \leqslant 2sm$. 由于 $f_1, \cdots, f_{s-1}, f_s'$ 都不为零，从而 A 的前 s 行中任意一行里，列指标为奇数的表值不为零，且任意两个相邻的非零表值相同.

设 $j_1 < \cdots < j_M$ 是 A 的前 s 行中所有零表值的列指标组成的 (偶数) 数列，则 $f_1, \cdots, f_{s-1}, f_s'$ 在 R 中的根共有 M 个. 从而可令这些根为 $\alpha_{j_1} < \alpha_{j_2} < \cdots < \alpha_{j_M}$.

若 $M = 0$, 则 f_s' 恒取正值或负值. 此时，f_s' 的次数显然为偶数, 从而 f_s 的次数为奇数. 因而 f_s 在 R 中有根. 另一方面，由引理 2.4.2 知，f_s 是单调的，从而在 R 中至多有一个根. 于是 f_s 在 R 中恰有一个根 α. 由此可知，$\mathrm{SGN}_R(f_1, \cdots, f_{s-1}, f_s)$ 是一个 $s \times 3$ 矩阵，其中第 i 行元素为

$$\mathrm{sgn}\big(f_i(]-\infty, \alpha[)\big), \mathrm{sgn}\big(f_i(\alpha)\big), \mathrm{sgn}\big(f_i(]\alpha, +\infty[)\big),$$

这里 $i = 1, \cdots, s$. 由 π 的规定可知，$\pi(A) = \mathrm{SGN}_R(f_1, \cdots, f_s)$.

现设 $M > 0$. 由前面的讨论知，存在 $\{1, \cdots, M\}$ 到 $\{1, \cdots, s\}$ 的一个映射 θ, 使得对于每个 $k \in \{1, \cdots, M\}$, $a_{\theta(k), j_k} = 0$, 即 $h_{\theta(k)}(\alpha_{j_k}) = 0$, 这里约定 $h_i = f_i, i = 1, \cdots, s-1$, 而 $h_s = f_s'$. 注意到 $g_{\theta(k)}$ 是 $h_{\theta(k)}$ 除 f_s 的余式, 从而 $f_s(\alpha_{j_k}) = g_{\theta(k)}(\alpha_{j_k})$.

由引理 2.4.2 知，f_s 在 $]-\infty, \alpha_{j_1}[,]\alpha_{j_1}, \alpha_{j_2}[, \cdots,]\alpha_{j_{M-1}}, \alpha_{j_M}[,]\alpha_{j_M}, +\infty[$ 中每个开区间中至多有一个根. 分别讨论下列情况:

(1) 对于每对数 (j_k, j_{k+1}), $k = 1, \cdots, M-1$, 若 $a_{s+\theta(k), j_k} \cdot a_{s+\theta(k+1), j_{k+1}} = -1$, 即 $\mathrm{sgn}\big(g_{\theta(k)}(\alpha_{j_k})\big)\mathrm{sgn}\big(g_{\theta(k+1)}(\alpha_{j_{k+1}})\big) = -1$, 则 $f_s(\alpha_{j_k})$ 和 $f_s(\alpha_{j_{k+1}})$ 异号. 从而 f_s 在 $]\alpha_{j_k}, \alpha_{j_{k+1}}[$ 中有一个根，且记作 α_{j_k+1}. 否则，f_s 在 $]\alpha_{j_k}, \alpha_{j_{k+1}}[$ 中无根.

(2) 若 $a_{s,1} \cdot a_{s+\theta(1), j_1} = -1$, 即 $\mathrm{sgn}\big(f_s'(]-\infty, \alpha_{j_1}[)\big)$ 和 $\mathrm{sgn}\big(g_{\theta(1)}(\alpha_{j_1})\big)$ 异号，则 $\mathrm{sgn}\big(f_s'(]-\infty, \alpha_{j_1}[)\big) \cdot \mathrm{sgn}\big(f_s(\alpha_{j_1})\big) = -1$. 此时易知，$f_s$ 在 $]-\infty, \alpha_{j_1}[$ 中有一个根，且记作 α_{j_1-1}. 否则，f_s 在 $]-\infty, \alpha_{j_1}[$ 中无根.

(3) 若 $a_{s,2t+1} \cdot a_{s+\theta(M), j_M} = -1$, 则同样可知，$f_s$ 在 $]\alpha_{j_M}, +\infty[$ 中有一个根，且记作 α_{j_M+1}. 否则，f_s 在 $]\alpha_{j_M}, +\infty[$ 中无根.

这表明：通过对数列：$j_1 < \cdots < j_M$ 进行如上处理，该数列因插入奇数而扩充为新数列 $r_1 < \cdots < r_n$, 其中 $M \leqslant N$, 使得 $\alpha_{r_1}, \cdots, \alpha_{r_N}$ 恰为 $f_1, \cdots, f_{s-1}, f_s'$ 和 f_s 在 R 中的全部根，且 $f_s(\alpha_{r_e}) = 0$, 只要 r_e 为奇数.

据此，可构造一个 $s \times (2N+1)$ 矩阵，使得第 i 行中表值为

$$\mathrm{sgn}\big(f_i(]-\infty, \alpha_{r_1}[)\big), \mathrm{sgn}\big(f_i(\alpha_{r_1})\big), \mathrm{sgn}\big(f_i(]\alpha_{r_1}, \alpha_{r_2}[)\big), \cdots, \mathrm{sgn}\big(f_i(\alpha_{r_N})\big),$$
$$\mathrm{sgn}\big(f_i(]\alpha_{r_N}, +\infty[)\big).$$

与前面的讨论相对照，不难验证：所构造的矩阵恰为 A_1.

再由引理 7.2.2 知，$\mathrm{SGN}_R(f_1, \cdots, f_s) = A_2$, 这里 A_2 是 A_1 通过 "划去相邻的相同列" 所得的矩阵. 此时必有，$A_2 \in W_{s,m}$. 由前面的规定知，$\mathrm{SGN}_R(f_1, \cdots, f_s) = \pi(A) = \mathrm{SGN}_R(f_1, \cdots, f_{s-1}, f_s', g_1, \cdots, g_s)$. 证毕.

现考虑由全体 (无序的) 非负整数组构成的集合:

$$\Xi = \{(m_1, \cdots, m_r) \mid r \text{ 为自然数}, \quad m_i \text{ 为非负整数}, \quad i = 1, \cdots, r\}.$$

对于 $\sigma = (m_1, \cdots, m_r)$, $\tau = (m'_1, \cdots, m'_s) \in \Xi$, $\sigma = \tau$ 意指每个非负整数在 σ 和 τ 中出现的次数相同. 此外, 规定 $\sigma \prec \tau$, 如果有某个非负整数 k, 使得 k 在 σ 中出现的次数小于 k 在 τ 中出现的次数, 且每个大于 k 的整数在 σ 和 τ 中出现的次数相同. 容易证明所规定的二元关系 $\prec$ 是集 Ξ 的一个良序.

现在, 我们可以证明下面命题.

命题 7.2.4 设 $f_i(x; Y) = h_{i,m_i}(Y)x^{m_i} + h_{i,m_i-1}(Y)x^{m_i-1} + \cdots + h_{i,0}(Y)$ 是 $n+1$ 元整系数多项式, $i = 1, \cdots, s$, 其中 $Y = (y_1, \cdots, y_n)$ 是由 n 个变量组成的变量组. 如果 W' 是 $W_{s,m}$ 的一个子集, 那么存在有限个由形如 $g(Y) = 0$ 的方程以及形如 $g(Y) < 0$ 的不等式构成的关系式组 $S_1, \cdots, S_r$, 其中 $g(Y) \in \mathbb{Z}[Y]$, 使得对于每个实闭域 R 以及任意 $\bar{a} = (a_1, \cdots, a_n) \in R^n$, $\mathrm{SGN}_R(f_1(x; \bar{a}), \cdots, f_s(x; \bar{a})) \in W'$, 当且仅当 $\bar{a}$ 满足 $S_1, \cdots, S_r$ 中某个关系式组.

证明 不失一般性, 可假定所讨论的多项式 $f_1, \cdots, f_s$ 都不为零, 且每个 $h_{i,m_i}(Y)$ 也不恒为零, $i = 1, \cdots, s$.

假定命题不成立, 则集 Ξ 的如下子集非空:

$$\mathcal{L} = \{(\deg(f_1; x), \cdots, \deg(f_s; x)) \mid f_1, \cdots, f_s \in \mathbb{Z}[x; Y], \text{使得命题不成立}\},$$

这里 $\deg(f_i; x)$ 表示多项式 f_i 关于变量 x 的次数, $i = 1, \cdots, s$. 由于 $\prec$ 是 Ξ 的一个良序, 从而可选取一组多项式 $f_1, \cdots, f_s \in \mathbb{Z}[x]$, 使得 $(m_1, \cdots, m_s) = (\deg(f_1; x), \cdots, \deg(f_s; x))$ 是 $\mathcal{L}$ 中关于 $\prec$ 的最小元素, 且命题对于 $f_1, \cdots, f_s$ 不成立.

令 $m = \max\{m_1, \cdots, m_s\}$. 若 $m = 0$, 则 $f_1, \cdots, f_s \in \mathbb{Z}[Y]$. 此时, 对于每个 $s \times 1$ 矩阵 $w \in W'$, 矩阵等式

$$\begin{pmatrix} \mathrm{sgn}(f_1) \\ \vdots \\ \mathrm{sgn}(f_s) \end{pmatrix} = w$$

相当于一个由 s 个方程或不等式组成的关系式组 S_w. 记 W'_0 是 W' 中所有 $s \times 1$ 矩阵组成的子集. 当 $W'_0 \neq \emptyset$ 时, 取关系式组 S_w, $w \in W'_0$; 而当 $W'_0 = \emptyset$ 时, 取 $S_1 = \{1 = 0\}$. 此时易知, 对于每个实闭域 R 以及任意 $\bar{a} = (a_1, \cdots, a_n) \in R^n$, $\mathrm{SGN}_R(f_1(x; \bar{a}), \cdots, f_s(x; \bar{a})) \in W'$, 当且仅当 $\bar{a}$ 满足所取的某个关系式组, 这矛盾于多项式组 $f_1, \cdots, f_s$ 的选取.

若 $m \geqslant 1$, 则可设 $m_s = m$. 设 f'_s 是 f_s 关于 x 的偏导数. 此外, 由环 $\mathbb{Z}[Y]$ 上一元多项式的带余除法知, 对于充分大的正偶数 e, 下列等式成立:

$$h^e_{i,m_i} f_s = q_i f_i + g_i, \; i = 1, \cdots, s-1;$$

$$(m_s h_{s,m_s})^e f_s = q_s f_s' + g_s,$$

其中 $q_i, g_i \in \mathbb{Z}[x;Y], i=1, \cdots, s$.

设 π 是命题 7.2.3 中所示的 $W_{2s,m}$ 到 $W_{s,m}$ 的一个映射，且令 $W=\pi^{-1}(W')$ 是 W' 在映射 π 下的原象. 由命题 7.2.3 知，对于每个实闭域 R 及 R^n 中任意使得 $h_{i,m_i}(\bar{a}) \neq 0$ $(i=1, \cdots, s)$ 的 $\bar{a}$,

$$\mathrm{SGN}_R\big(f_1(x,\bar{a}), \cdots, f_{s-1}(x;\bar{a}), f_s(x;\bar{a})\big) \in W',$$

当且仅当

$$\mathrm{SGN}_R\big(f_1(x,\bar{a}), \cdots, f_{s-1}(x;\bar{a}), f_s'(x;\bar{a}), g_1(x;\bar{a}), \cdots, g_s(x;\bar{a})\big) \in W.$$

注意到,

$$\begin{aligned}&\big(\deg(f_1;x), \cdots, \deg(f_{s-1};x), \deg(f_s';x), \deg(g_1;x), \cdots, \deg(g_s;x)\big)\\&\prec (m_1, \cdots, m_s).\end{aligned}$$

由 $(m_1, \cdots, m_s)$ 在 $\mathcal{L}$ 中的最小性知，命题结论对于多项式组： $f_1, \cdots, f_{s-1}, f_s'$, $g_1, \cdots, g_s$ 成立. 从而有欲求的关系式组 $S_1', \cdots, S_r'$, 使得对于每个实闭域 R 以及任意 $\bar{a} \in R^n$, $\mathrm{SGN}_R\big(f_1(x,\bar{a}), \cdots, f_{s-1}(x;\bar{a}), f_s'(x;\bar{a}), g_1(x;\bar{a}), \cdots, g_s(x;\bar{a})\big) \in W$, 当且仅当 $\bar{a}$ 满足 $S_1', \cdots, S_r'$ 中某个关系式组.

再记 $e_i = f_i - h_{i,m_i}x^{m_i}$, $i=1, \cdots, s$. 此时显然有

$$\begin{aligned}&\big(\deg(f_1;x), \cdots, \deg(f_{i-1};x), \deg(e_i;x), \deg(f_{i+1};x), \cdots, \deg(f_s;x)\big)\\&\prec (m_1, \cdots, m_s).\end{aligned}$$

于是，命题的结论对于多项式组 $f_1, \cdots, f_{i-1}, e_i, f_{i+1}, \cdots, f_s$ 成立. 从而有如命题所求的关系式组 $S_{i,1}', \cdots, S_{i,r_i}'$, 使得对于每个实闭域 R 以及任意 $\bar{a} \in R^n$,

$$\mathrm{SGN}_R\big(f_1(x,\bar{a}), \cdots, f_{i-1}(x;\bar{a}), e_i(x;\bar{a}), f_{i+1}(x;\bar{a}), \cdots, f_s(x;\bar{a})\big) \in W',$$

当且仅当 $\bar{a}$ 满足 $S_{i,1}', \cdots, S_{i,r_i}'$ 中某个关系式组. 令 $S_{i,j_i} = S_{i,j_i}' \cup \{h_{i,m_i}=0\}$, $i=1, \cdots, s$; $j_i = 1, \cdots, r_i$, 且 $S_k = S_k' \cup \{-h_{i,m_i}^2 < 0 \mid 1 \leqslant i \leqslant r\}$. 由上面讨论可知，对于每个实闭域 R 以及任意 $\bar{a} \in R^n$, $\mathrm{SGN}_R\big(f_1(x,\bar{a}), \cdots, f_s(x;\bar{a})\big) \in W'$, 当且仅当 $\bar{a}$ 满足诸关系式组 S_k $(k=1, \cdots, r)$ 和 S_{i,j_i} $(i=1, \cdots, s;\ j_i=1, \cdots, r_i)$ 中的某组；这矛盾于 $f_1, \cdots, f_s$ 的选取. 因此，命题获证.

现然，很容易建立下面定理，这一定理被称作 Tarski-Seidenberg 原理 .

定理 7.2.5 设 $f_i(x;Y) = h_{i,m_i}(Y)x^{m_i} + h_{i,m_i-1}(Y)x^{m_i-1} + \cdots + h_{i,0}(Y)$ 是 $n+1$ 元整系数多项式， $i=1, \cdots, s$, 其中 $Y=(y_1, \cdots, y_n)$. 如果 ϵ 是 $\{1, \cdots, s\}$ 到 $\{-1,0,1\}$ 的一个映射，那么存在有限个由形如 $g(Y)=0$ 的方程以及形如 $g(Y)<0$ 的不等式所构成的关系式组 $S_1, \cdots, S_r$, 其中 $g(Y) \in \mathbb{Z}[Y]$, 使得对于每个实闭域 R

以及任意 $\bar{a}=(a_1,\cdots,a_n)\in R^n$, 关系式组

$$\begin{cases} \mathrm{sgn}\big(f_1(x;\bar{a})\big) &= \epsilon(1) \\ \mathrm{sgn}\big(f_2(x;\bar{a})\big) &= \epsilon(2) \\ \cdots\cdots \\ \mathrm{sgn}\big(f_s(x;\bar{a})\big) &= \epsilon(s) \end{cases}$$

在 R 中有解，当且仅当 $\bar{a}$ 满足 $S_1,\cdots,S_r$ 中某个关系式组.

证明 由引理 7.2.1 知，有 $W_{s,m}$ 的一个子集 $W(\epsilon)$, 使得对于每个实闭域 R 以及任意 $\bar{a}\in R^n$, 定理中的关系式组在 R 中有解，当且仅当

$$\mathrm{SGN}_R\big(f_1(x;\bar{a}),\cdots,f_s(x;\bar{a})\big)\in W(\epsilon).$$

再由命题 7.2.4 知, 存在有限个如命题所求的关系式组 $S_1,\cdots,S_r$, 使得对于每个实闭域 R 以及任意 $\bar{a}\in R^n$, $\mathrm{SGN}_R\big(f_1(x;\bar{a}),\cdots,f_s(x;\bar{a})\big)\in W(\epsilon)$, 当且仅当 $\bar{a}$ 满足 $S_1,\cdots,S_r$ 中某个关系式组. 因此, $S_1,\cdots,S_r$ 为所求的关系式组. 证毕.

推论 设 F 是一个实域, $f_1(x;Y),\cdots,f_s(x;Y)\in F[x;Y]$ 是 F 上 $n+1$ 元多项式, 其中 $Y=(y_1,\cdots,y_n)$. 如果 ϵ 是 $\{1,\cdots,s\}$ 到 $\{-1,0,1\}$ 的一个映射, 那么存在有限个由形如 $g(Y)=0$ 的方程以及形如 $g(Y)<0$ 的不等式组成的关系式组 $S_1,\cdots,S_r$, 其中 $g(Y)\in F[Y]$, 使得对于每个包含 F 的实闭域 R 以及任意 $\bar{a}\in R^n$, 关系式组

$$\begin{cases} \mathrm{sgn}\big(f_1(x;\bar{a})\big) &= \epsilon(1) \\ \mathrm{sgn}\big(f_2(x;\bar{a})\big) &= \epsilon(2) \\ \cdots\cdots \\ \mathrm{sgn}\big(f_s(x;\bar{a})\big) &= \epsilon(s) \end{cases}$$

在 R 中有解，当且仅当 $\bar{a}$ 满足 $S_1,\cdots,S_r$ 中某个关系式组.

证明 设 $f_1,\cdots,f_s$ 在 F 中的全部系数依次为 $d_1,\cdots,d_m$, 且 $Z=(z_1,\cdots,z_m)$ 为相应的一组新变量, 则有 $H_i(x;Y;Z)\in\mathbb{Z}[x;Y;Z]$, 使得

$$f_i(x;Y)=H_i(x;Y;\bar{d}),\ i=1,\cdots,s,$$

其中 $\bar{d}:=(d_1,\cdots,d_m)$.

由定理 7.2.5, 存在有限个由形如 $g(Y;Z)=0$ 的方程以及形如 $g(Y;Z)<0$ 的不等式所构成的关系式组 $S_1',\cdots,S_r'$, 使得对于每个实闭域 R 以及任意 $\bar{a}\in R^n$ 和 $\bar{b}\in R^m$, 关系式组

$$\begin{cases} \operatorname{sgn}\big(H_1(x;\bar{a};\bar{b})\big) &= \epsilon(1) \\ \operatorname{sgn}\big(H_2(x;\bar{a};\bar{b})\big) &= \epsilon(2) \\ \cdots\cdots \\ \operatorname{sgn}\big(H_s(x;\bar{a},\bar{b})\big) &= \epsilon(s) \end{cases}$$

在 R 中有解，当且仅当 $Y = \bar{a}$, $Z = \bar{b}$ 是 $S'_1, \cdots, S'_r$ 中某个关系式组的解. 设 S_i 是 S'_i 中全部关系式通过代换 $Z = \bar{d}$ 转化而成的关系式组， $i = 1, \cdots, s$, 则显然 $S_1, \cdots, S_r$ 满足推论的要求.

§7.3 转 移 定 理

在本节中，借助于 Tarski-Seidenberg 原理，我们将证明这样一个重要事实：极大序域类容许量词消去. 在此基础上，有重要应用意义的转移定理被建立.

从 §7.1 中例 2 可知，所有极大序域组成的类是初等类. 在本节中，用 $K^<$ 表示所有极大序域组成的类. 为简便起见，$K^<$ 中的每个结构只写作二要素组合 $(R, <)$, 其中 R 是一个实闭域， $<$ 是 R 的惟一序.

为简便起见,对于一个常量项 $t \in \mathrm{Tm}_n$ 以及自然数 m, 约定: mt 表示 $t+t+\cdots+t$ (m 个 t), 而 $-mt$ 表示 $(-t)+\cdots+(-t)$ (m 个 $-t$). 这样, 多项式环 $\mathbb{Z}[c_1, c_2, \cdots, c_n]$ 中每个多项式都是 Tm_n 中一个项. 记 $F_n^<$ 是由 $C_n^<$ 中所有这样的结构 $(\mathcal{A}, a_1, \cdots, a_n)$ 组成的类，其中 $\mathcal{A}$ 是序域类中一个结构， $a_1, \cdots, a_n \in |\mathcal{A}|$. 根据常量项在结构中的解释可知， $\mathrm{Tm}_n^<$ 中每个常量项都与一个含常量符号 $c_1, \cdots, c_n$ 的整系数多项式在 $F_n^<$ 的所有结构中具有相同的解释. 显然，对于任意两个常量项 $t_1, t_2 \in \mathrm{Tm}_n$, 原始公式 $t_1 = t_2$ 和 $t_1 < t_2$ 模于 $F_n^<$ 分别等价于 $t_1 - t_2 = 0$ 和 $t_1 - t_2 < 0$. 注意到， $t_1 - t_2$ 是 Tm_n 中常量项. 因此，模于 $F_n^<$, 每个仅含常量符号的原始公式等价于 $f(c_1, \cdots, c_n) = 0$ 或 $f(c_1, \cdots, c_n) < 0$, 这里 $f(c_1, \cdots, c_n) \in \mathbb{Z}[c_1, \cdots, c_n]$.

形如 $f_i(c_1, \cdots, c_n) = 0$ 或 $f_i(c_1, \cdots, c_n) < 0$ 的语句称作原始语句, 如果 $f(c_1, \cdots, c_n) \in \mathbb{Z}[c_1, \cdots, c_n]$. 若 γ_i 为原始语句， $i = 1, \cdots, s$, 则语句 $\gamma_1 \wedge \cdots \wedge \gamma_s$ 称作原始语句的一个合取.

引理 7.3.1 设 $\gamma \in \Gamma_n^<$, 则模于 $F_n^<$, γ 等价于这样形式的语句： $\gamma_1 \vee \gamma_2 \vee \cdots \vee \gamma_r$, 这里 γ_i 是原始语句的一个合取， $i = 1, \cdots, r$.

证明 用 $\ell(\gamma)$ 表示 γ 中所含字符的总数. 下面对 $\ell(\gamma)$ 施用第二归纳法来证明引理.

设 k 为自然数，且假定对于 $\Gamma_n^<$ 中每个使得 $\ell(\gamma) < k$ 的语句 γ, 上面的引理成立. 现设 $\phi \in \Gamma_n^<$, 且 $\ell(\phi) = k$. 由序域语言中公式的定义知， ϕ 具有如下四种形式：

(1)ϕ 为原始公式. 此时，由上面讨论知， ϕ 模于 $F_n^<$ 等价于原始语句

$$f(c_1, \cdots, c_n) = 0 \text{ 或 } f(c_1, \cdots, c_n) < 0,$$

其中 $f(c_1, \cdots, c_n) \in \mathbb{Z}[c_1, \cdot \cdots, c_n]$.

(2)ϕ 为 $\gamma_1 \vee \gamma_2$, 其中 $\gamma_1, \gamma_2 \in \Gamma_n^<$. 注意到, $\ell(\gamma_1) < k$ 且 $\ell(\gamma_2) < k$. 由归纳假定知，模于 $F_n^<$, γ_1 和 γ_2 都分别等价于引理中所示的语句. 从而 ϕ 也等价于引理中所示的语句.

(3)ϕ 为 $\gamma_1 \wedge \gamma_2$, 其中 $\gamma_1, \gamma_2 \in \Gamma_n^<$. 由归纳假定可知，模于 $F_n^<$, γ_i 等价于 $\gamma_{i1} \vee \gamma_{i2} \vee \cdots \vee \gamma_{ir_i}$, 其中 γ_{ij_i} 是原始语句的一个合取， $i = 1, 2; j_i = 1, 2, \cdots, n_i$. 此时， ϕ 模于 $F_n^<$ 等价于如下语句

$$(\gamma_{11} \wedge \gamma_{21}) \vee \cdots \vee (\gamma_{11} \wedge \gamma_{2n_2}) \vee \cdots \vee (\gamma_{1n_1} \wedge \gamma_{21}) \vee \cdots \vee (\gamma_{1n_1} \wedge \gamma_{2n_2}),$$

其中每个括号中的语句都是原始语句的一个合取.

(4)ϕ 为 $\sim \gamma$. 当 γ 为原始公式时，由上面讨论知， γ 模于 $F_n^<$ 等价于原始语句 $f(c_1, \cdots, c_n) = 0$ 或 $f(c_1, .., c_n) < 0$. 此时， ϕ 模于 $F_n^<$ 等价于 $f_1(c_1, \cdots, c_n) < 0 \vee -f(c_1, \cdots, c_n) < 0$ 或 $f(c_1, \cdots, c_n) = 0 \vee -f(c_1, \cdots, c_n) < 0$. 当 γ 为 $\gamma_1 \vee \gamma_2$ 时，其中 $\gamma_1, \gamma_2 \in \Gamma_n^<$, ϕ 模于 $F_n^<$ 等价于 $\sim \gamma_1 \wedge \sim \gamma_2$. 由于 $\ell(\gamma_1)$ 和 $\ell(\gamma_2)$ 都小于 k, 从而由情况 (3) 的讨论知， ϕ 等价于引理中所示的语句. 当 ϕ 为 $\gamma_1 \wedge \gamma_2$ 时，其中 $\gamma_1, \gamma_2 \in \Gamma_n^<$, ϕ 等价于 $\sim \gamma_1 \vee \sim \gamma_2$. 此时，由情况 (2) 的讨论知， ϕ 等价于引理中所示的语句.

由归纳原理，上面的引理获证. 证毕.

引理 7.3.2 设 $\gamma \in \Gamma_n^<$, 其中 n 为正整数，则有某个 $\gamma' \in \Gamma_{n-1}^<$, 使得对于每个 $(R, <) \in K^<$ 以及任意 $a_1, \cdots, a_{n-1} \in R$, $(R, <, a_1, \cdots, a_{n-1}) \models \gamma'$, 当且仅当存在某个 $a_n \in R$, 满足 $(R, <, a_1, \cdot \cdots, a_n) \models \gamma$.

证明 由引理 7.3.1 知， γ 模于 $F_n^<$ 等价于如下语句:

$$\gamma_1 \vee \cdots \vee \gamma_r,$$

这里 γ_i 是原始语句的一个合取， $i = 1, \cdots, r$.

对于每个 $i = 1, \cdots, r$, 设 γ_i 为 $\gamma_{i1} \wedge \cdots \wedge \gamma_{is_i}$, 其中 γ_{ij} 为原始语句: $f_{ij}(c_1, \cdots, c_n) = 0$ 或 $f_{ij}(c_1, \cdots, c_n) < 0$, $j = 1, \cdots, s_i$. 记 $\epsilon_{ij} = 0$ 或 -1, 根据 γ_{ij} 为 $f_{ij}(c_1, \cdots, c_n) = 0$ 或 $f_{ij}(c_1, \cdots, c_n) < 0$ 而定. 考察如下关系式组:

$$\operatorname{sgn}(f_{ij}(c_1, \cdots, c_n)) = \epsilon_{ij}, \quad j = 1, \cdots, s_i.$$

由 Tarski-Seidenberg 原理知，存在有限个由形如 $g = 0$ 的方程以及形如 $g < 0$ 的不等式所构成的关系式组 $S_{i1}, \cdots, S_{it_i}$, 其中 $g \in \mathbb{Z}[c_1, \cdots, c_{n-1}]$, 使得对于每个实闭域 R 以及任意 $(a_1, \cdots, a_{n-1}) \in R^{n-1}$, 关系式组 $\operatorname{sgn}(f_{ij}(a_1, \cdots, a_{n-1}, c_n)) = \epsilon_{ij}$, $j = 1, \cdots, s_i$ 在 R 中有解，当且仅当 $(a_1, \cdots, a_{n-1})$ 满足 $S_{i1}, \cdots, S_{it_i}$ 中某个关系式组.

显然, S_{ik} $(k=1,\cdots,t_i)$ 中每个关系式可看作 $\Gamma_{n-1}^{<}$ 中一个原始语句. 从而关系组 S_{ik} 可看作原始语句的一个合取 ψ_{ik}, $k=1,\cdots,t_i$. 令 $\phi_i=\psi_{i1}\vee\cdots\vee\psi_{it_i}$, 则 $\phi_i\in\Gamma_{n-1}^{<}$, $i=1,\cdots,r$.

再令 $\gamma'=\phi_1\vee\cdots\vee\phi_r$, 则 $\gamma'\in\Gamma_{n-1}^{<}$. 此时易见, γ' 为定理所要求的语句.

根据引理 7.3.2, 容易证明下面的重要定理.

定理 7.3.3 所有极大序域组成的类 $K^{<}$ 容许量词消去.

证明 假定上面定理不成立, 则可选取这样的一个 $\phi\in\mathrm{Sent}_n^{<}$, 使得对于每个 $\gamma\in\Gamma_n^{<}$, 总有某个 $(R,<)\in K^{<}$ 以及某些 $a_1,\cdots,a_n\in R$, 导致关系式: $(R,<,a_1,\cdots,a_n)\models(\phi\longleftrightarrow\gamma)$ 不成立, 且 ϕ 所含的字符最少.

显然, ϕ 不可能为原始公式; 否则, $\phi\in\Gamma_n^{<}$. 根据序域语言中公式的定义可知, ϕ 可能有如下形式:

(1)ϕ 为 $\sim\psi$, 其中 $\psi\in\mathrm{Sent}_n^{<}$. 由于 ψ 所含的字符少于 ϕ 所含的字符, 从而由 ϕ 的选取知, 有 $\gamma_1\in\Gamma_n^{<}$, 使得对于每个 $(R,<)\in K^{<}$ 以及任意 $a_1,\cdots,a_n\in R$, $(R,<,a_1,\cdots,a_n)\models(\psi\longleftrightarrow\gamma_1)$. 令 γ 为 $\sim\gamma_1$, 则 $\gamma\in\Gamma_n^{<}$. 此时, 显然有 $(R,<,a_1,\cdots,a_n)\models(\phi\longleftrightarrow\gamma)$, 这矛盾于 ϕ 的选取.

(2)ϕ 为 $\phi_1\wedge\phi_2$ 或 $\phi_1\vee\phi_2$, 其中 $\phi_1,\phi_2\in\mathrm{Sent}_n^{<}$. 此时易知, 有 $\gamma_1,\gamma_2\in\Gamma_n^{<}$, 使得对于每个 $(R,<)\in K^{<}$ 以及任意 $a_1,\cdots,a_n\in R$, $(R,<,a_1,\cdots,a_n)\models(\phi_i\longleftrightarrow\gamma_i)$, $i=1,2$. 由此有 $(R,<,a_1,\cdots,a_n)\models(\phi\longleftrightarrow\gamma_1\wedge\gamma_2)$, 或 $(R,<,a_1,\cdots,a_n)\models(\phi\longleftrightarrow\gamma_1\vee\gamma_2)$. 注意到 $\gamma_1\wedge\gamma_2$, $\gamma_1\vee\gamma_2\in\Gamma_n^{<}$, 从而上面表达式矛盾于 ϕ 的选取.

(3)ϕ 为 $\exists x\psi(x)$, 其中 $\psi(x)\in\mathrm{Fml}_n^{<}$ 是含有变量符号 x 的一个公式. 此时, $\psi(c_{n+1})\in\mathrm{Sent}_{n+1}^{<}$, 且它所含的字符少于 ϕ 所含的字符. 由 ϕ 的选取可知, 有 $\gamma_1\in\Gamma_{n+1}^{<}$, 使得对于每个 $(R,<)\in K^{<}$ 以及任意 $a_1,\cdots,a_{n+1}\in R$, $(R,<,a_1,\cdots,a_{n+1})\models(\psi(c_{n+1})\longleftrightarrow\gamma_1)$.

由引理 7.3.2 知, 有 $\gamma\in\Gamma_n^{<}$, 使得对于每个 $(R,<)\in K^{<}$ 以及任意 $a_1,\cdots,a_n\in R$, $(R,<,a_1,\cdots,a_n)\models\gamma$, 当且仅当存在某个 $a_{n+1}\in R$, 使得 $(R,<,a_1,\cdots,a_n,a_{n+1})\models\gamma_1$. 由此可知, 对于每个 $(R,<)\in K^{<}$ 以及任意 $a_1,\cdots,a_n\in R$, $(R,<,a_1,\cdots,a_n)\models(\phi\longleftrightarrow\gamma)$, 矛盾于 ϕ 的选取.

(4)ϕ 为 $\forall x\psi(x)$, 其中 $\psi(x)\in\mathrm{Fml}_n^{<}$ 是含有变量符号 x 的一个公式. 此时, ϕ 等价于语句: $\sim\exists x(\sim\psi(x))$. 显然 $\sim\psi(c_{n+1})\in\mathrm{Sent}_{n+1}^{<}$, 且它所含的字符少于 ϕ 所含的字符. 根据情况 (3) 的类似讨论, 有 $\gamma\in\Gamma_n^{<}$, 使得对于每个 $(R,<)\in K^{<}$ 以及任意 $a_1,\cdots,a_n\in R$, $(R,<,a_1,\cdots,a_n)\models\gamma$, 当且仅当存在某个 $a_{n+1}\in R$, 使得 $(R,<,a_1,\cdots,a_n,a_{n+1})\models\sim\psi(c_{n+1})$. 于是, $\sim\gamma\in\Gamma_n^{<}$, 且对于每个 $(R,<)\in K^{<}$ 以及任意 $a_1,\cdots,a_n\in R$, $(R,<,a_1,\cdots,a_n)\models(\phi\longleftrightarrow\sim\gamma)$, 矛盾于 ϕ 的选取.

综上所述, 定理 7.3.3 获证. 证毕.

由定理 7.3.3, 容易推出下面的两个结论.

定理 7.3.4 设 R 和 R' 是两个实闭域，且 $R \subseteq R'$, 则 $(R,<) \preceq (R',<')$, 这里 $<$ 和 $<'$ 分别为 R 和 R' 的惟一序.

证明 由命题 2.3.2 的推论知，$(R,<)$ 是 $(R',<')$ 的一个子结构，即 $(R,<) \subseteq (R',<')$. 再由定理 7.3.3 和命题 7.1.1 知，$(R,<) \preceq (R',<')$. 证毕.

定理 7.3.5 设 R 和 R' 都为实闭域，$<$ 和 $<'$ 分别为 R 和 R' 的惟一序，则 $(R,<) \equiv (R',<')$.

证明 注意到，有理数域 $\mathbb{Q}$ 可看作 R 和 R' 的共同子域. 令 $\widetilde{\mathbb{Q}}$ 和 $\widetilde{\mathbb{Q}}'$ 分别为 $\mathbb{Q}$ 在 R 和 R' 中的代数闭包. 由命题 2.1.5 可知，$\widetilde{\mathbb{Q}}$ 和 $\widetilde{\mathbb{Q}}'$ 都是序域 $(\mathbb{Q},\mathbb{Q}^2)$ 的实闭包. 由实闭包的惟一性 (定理 2.3.6), 可认定 $\widetilde{\mathbb{Q}}' = \widetilde{\mathbb{Q}}$. 此时有 $\widetilde{\mathbb{Q}} \subseteq R$, 且 $\widetilde{\mathbb{Q}} \subseteq R'$. 记 $<_0$ 为 $\widetilde{\mathbb{Q}}$ 的惟一序. 由定理 7.3.4 知 $(\widetilde{\mathbb{Q}},<_0) \preceq (R,<)$, 且 $(\widetilde{\mathbb{Q}},<_0) \preceq (R',<')$. 由 "初等子结构" 的定义可知，$(\widetilde{\mathbb{Q}},<_0) \equiv (R,<)$, 且 $(\widetilde{\mathbb{Q}},<_0) \equiv (R',<')$. 从而有 $(R,<) \equiv (R',<')$. 证毕.

定理 7.3.5 常称作 Tarski 原理 . 作为定理 7.3.5 的一个应用, 我们证明这样一个事实: 实数序域 $(\mathbb{R},<)$ 的任意一个泛初等性质同样适合所有的序域. $(\mathbb{R},<)$ 的一个泛初等性质是指 $\mathrm{Sent}_0^{\leq}$ 中一个语句 ϕ, 使得 $(\mathbb{R},<) \models \phi$, 且 ϕ 为 $\forall x_1 \cdots \forall x_n \psi(x_1,\cdots,x_n)$, 这里 $\psi(x_1,\cdots,x_n)$ 是 $\mathrm{Fml}_0^{\leq}$ 中一个无量词的公式.

定理 7.3.6 实数序域 $(\mathbb{R},<)$ 的任意一个泛初等性质适合于所有的序域.

证明 设 $(F,<)$ 是任意一个序域. 记 R 为 $(F,<)$ 的实闭包，且 R 的惟一序仍记作: $<$. 设 ϕ 是 $(\mathbb{R},<)$ 的任意一个泛初等性质，则 $(\mathbb{R},<) \models \phi$. 由定理 7.3.5 知, $(R,<) \models \phi$. 注意到，若一个泛初等性质在某个结构中成立，则这个泛初等性质适合于该结构的所有子结构. 因此，$(F,<) \models \phi$. 证毕.

为了应用的方便，我们需要一个更方便的结论 —— 转移定理. 在建立转移定理之前，我们需要引进一些有关概念.

设 $(F,<_F)$ 是一个序域. 将 F 中的全部元素作为常量符号扩充到序域语言中，所得的语言称作常量在 $(F,<_F)$ 中的序域语言，且记作: $\mathcal{L}(F,<_F)$. $\mathcal{L}(F,<_F)$ 的一个结构是这样一个序域 $(K,<)$, 使得 $(K,<)$ 是 $(F,<_F)$ 的一个序扩张. 按照 §7.1 中类似方式，我们可以定义语言 $\mathcal{L}(F,<_F)$ 中的项，公式和语句. 同样，我们可以规定一个语句在 $\mathcal{L}(F,<_F)$ 的任意一个结构中的解释，只需将该语句中常量符号看作 F 中元素 (也即该结构的域中元素). 于是，表达式 $(K,<) \models \phi$ 有自然明确的意义，其中 $(K,<)$ 是 $\mathcal{L}(F,<_F)$ 的一个结构，ϕ 是 $\mathcal{L}(F,<_F)$ 的一个语句.

现在，我们可以建立如下所谓的转移定理 .

定理 7.3.7 设 $(F,<_F)$ 是一个实闭包为 R 的序域，ϕ 是 $\mathcal{L}(F,<_F)$ 的一个语句，且 K 是 F 的一个实闭扩张，使得 K 的惟一序 $<$ 是序 $<_F$ 在 K 上的拓展，则 $(R,<_R) \models \phi$, 当且仅当 $(K,<) \models \phi$, 这里 $<_R$ 是 R 的惟一序.

证明 设 R_1 是 F 在 K 中的代数闭包. 由命题 2.1.5 知，R_1 也是序域 $(F,<_F)$

的实闭包．由实闭包的惟一性，可认定 $R_1 = R$. 从而 $R \subseteq K$. 根据定理 7.3.4, 有 $(R, <_R) \preceq (K, <)$.

设 $a_1, \cdots, a_n$ 是语句 ϕ 中所出现的全部常量 (即 F 中元素). 在语句 ϕ 中, 用常量符号 $c_1, \cdots, c_n$ 分别替换 $a_1, \cdots, a_n$, 则得 $\mathrm{Sent}_n^{<}$ 中一个语句 $\Psi(c_1, \cdots, c_n)$. 注意到, $a_1, \cdots, a_n \in R$. 由 $(R, <_R) \preceq (K, <)$ 知， $(R, <_R, a_1, \cdots, a_n) \models \Psi(c_1, \cdots, c_n)$ 当且仅当 $(K, <, a_1, \cdots, a_n) \models \Psi(c_1, \cdots, c_n)$. 这表明 $(R, <_R) \models \phi$ 当且仅当 $(K, <) \models \phi$. 证毕.

§7.4 点定理与隐函数定理

在本节中，将应用上节中有关定理来建立实域论和实代数几何中一些重要结论，这些结论包括正点定理，非负点定理，实零点定理和隐函数定理.

在建立点定理之前，我们需要进行一些预备工作. 这些预备工作是针对交换环的 “亚正锥” 而展开的. 因而，本节的 “环” 均指 “有单位元 1 的交换环”.

定义 7.4.1 设 A 是一个环. A 的一个子集 T 称作 A 的一个亚正锥，如果下列条件成立:

(1)$T + T \subseteq T$;

(2)$T \cdot T \subseteq T$;

(3)$-1 \notin T$;

(4)$A^2 \subseteq T$.

引理 7.4.1 设 T 是环 A 的一个亚正锥， $x \in A$, 使得对于每个自然数 n 以及每个 $t \in T$, $x(x^{2n} + t) \notin T$, 则 A 有一个亚正锥 P, 使得 $T \subseteq P$, $A = P \cup -P$, $P \cap -P$ 是 A 的一个素理想，且 $x \notin P$.

证明 设集合 Ξ 的成员为 A 的所有这样的亚正锥 S, 使得 S 满足下面条件:

$T \subseteq S$, 且对于每个自然数 n 和每个 $s \in S$, $x(x^{2n} + s) \notin S$.

显然， $T \in \Xi$, 且 Ξ 对于集合的包含关系是一个偏序集. 由 Zorn 引理可知, Ξ 中有极大元 P. 此时，我们有如下断言:

(1)$-x \in P$. 事实上，易知 $P - Px$ 满足定义 7.4.1 中条件 (1), (2) 和 (4). 如若 $-1 \in P - Px$, 则有 $p_1, p_2 \in P$, 使得 $-1 = p_1 - p_2 x$. 由此有 $x(x^2 + p_1 x^2) = p_2 x^4 \in P$, 且 $p_1 x^2 \in P$, 这矛盾于事实: $P \in \Xi$! 于是, $P - Px$ 是 A 的一个亚正锥. 假若对于某个自然数 k 以及某个 $y \in P - Px$, $x(x^{2k} + y) \in P - Px$, 则有 $x(x^{2k} + p_1 - p_2 x) = p_3 - p_4 x$, 其中 $p_i \in P$, $i = 1, 2, 3, 4$. 由此有 $x(x^{2k} + p_1 + p_4) = p_3 + p_2 x^2 \in P$, 矛盾. 这表明: $P - Px \in \Xi$. 注意到， $P \subseteq P - Px$. 由 P 在 Ξ 中的极大性知， $P = P - Px$. 因而， $-x \in P$.

(2) 对于每个 $a \in A$, $Pa \cap Q = \phi$ 或 $-Pa \cap Q = \phi$, 这里 $Q = \{x^{2n} + p \mid n \in \mathbb{N},$

$p \in P\}$. 事实上, 如若不然, 则有 $p_1, p_2, p_3, p_4 \in P$, 使得 $p_1 a = x^{2m} + p_2$, 且 $-p_3 a = x^{2n} + p_4$, 其中 $m, n \in \mathbb{N}$. 从而 $-p_1 p_3 a^2 = x^{2(m+n)} + p_2 x^{2n} + p_4 x^{2m} + p_2 p_4$, 即有 $x(x^{2(m+n)} + p_1 p_3 a^2 + p_2 x^{2n} + p_4 x^{2m} + p_2 p_4) = 0 \in P$, 矛盾.

由上面断言, 我们证明: 亚正锥 P 满足定理的条件.

先证: $A = P \cup -P$. 设 $a \in A$. 由断言 (2) 知, $Pa \cap Q = \phi$ 或 $-Pa \cap Q = \phi$. 当 $Pa \cap Q = \phi$ 时, 令 $P_1 = P - Pa$. 显然, P_1 满足定义 7.4.1 中条件 (1), (2) 和 (4). 如若 $-1 \in P_1$, 则 $-1 = p_1 - p_2 a$, 其中 $p_1, p_2 \in P$. 由此有 $(p_2 x^2)a = x^2 + p_1 x^2 \in Pa \cap Q$, 矛盾. 因而, P_1 是 A 的一个亚正锥. 假若对于某个自然数 k 以及某个 $y \in P_1$, $x(x^{2k} + y) \in P_1$, 则有 $x(x^{2k} + p_1 - p_2 a) = p_3 - p_4 a$, 其中 $p_i \in P$, $i = 1, 2, 3$ 和 4. 从而有 $(p_2 x^2 - p_4 x)a = x^{2(k+1)} + p_1 x^2 - p_3 x$. 由断言 (1) 知, $-x \in P$. 由此可知, $(p_2 x^2 - p_4 x)a \in Pa \cap Q$, 矛盾. 此时可知, $P_1 \in \Xi$, 且 $P \subseteq P_1$. 由 P 在 Ξ 中的极大性知, $P_1 = P$. 因而, $-a \in P_1 = P$. 当 $-Pa \cap Q = \phi$ 时, 同样可推出 $a \in P$.

再证 $P \cap -P$ 是 A 的一个素理想. 令 $J = P \cap -P$. 由 $A = P \cup -P$ 易知, J 是 A 的一个理想. 假若 J 不是 A 的素理想, 则有 $a, b \in A$, 使得 $ab \in J$, 但 $a, b \notin J$. 不失一般性, 不妨设 $a, b \notin -P$. 由前面的讨论知, $Pa \cap Q \neq \phi$ 且 $Pb \cap Q \neq \phi$. 从而有 $p_1, p_2, p_3, p_4 \in P$, 使得 $p_1 a = x^{2m} + p_2$, 且 $p_3 b = x^{2n} + p_4$, 其中 $m, n \in \mathbb{N}$. 由此有 $x(x^{2(m+n)} + p_2 x^{2n} + p_4 x^{2m} + p_2 p_4) = x p_1 p_2 (ab) \in J \subseteq P$, 矛盾. 因而, J 是 A 的一个素理想.

此外, 显然 $T \subseteq P$, 且 $x \notin P$. 证毕.

设 (F, P) 是一个序域, R 是 (F, P) 的实闭包, 且 $\leqslant$ 为 R 的惟一序. 对于 $F[x_1, \cdots, x_n]$ 中有限个多项式 $u_1, \cdots, u_r$ 和 $v_1, \cdots, v_s$, 用 U 表示 $F[x_1, \cdots, x_n]$ 中由 $u_1, \cdots, u_r$ 生成的乘法么半群, 而 W 表示 $F[x_1, \cdots, x_n]$ 中由 $u_1, \cdots, u_r$ 以及 $v_1, \cdots, v_s$ 生成的乘法么半群, 且构作 $F[x_1, \cdots, x_n]$ 的如下子集:

$$S(W) = \left\{ \sum_{i=1}^{m} p_i w_i g_i^2 \mid m \in \mathbb{N}, p_i \in P, w_i \in W, g_i \in F[x_1, \cdots, x_n], i = 1, \cdots, m \right\}.$$

显然, $W \subseteq S(W)$, 且 $S(W)$ 对于多项式的加法与乘法是封闭的.

定理 7.4.2(半代数正点定理) 所设同上, 且 I 是 $F[x_1, \cdots, x_n]$ 的一个理想, 则对于 $f \in F[x_1, \cdots, x_n]$, 下列叙述等价:

(1) 对于 $a_1, \cdots, a_n \in R$, $f(a_1, \cdots, a_n) > 0$, 只要 $u_i(a_1, \cdots, a_n) > 0$, $i = 1, \cdots, r$, $v_j(a_1, \cdots, a_n) \geqslant 0$, $j = 1, \cdots, s$, 且对于每个 $h \in I$, $h(a_1, \cdots, a_n) = 0$;

(2) 存在 $s_1, s_2 \in S(W)$ 以及 $u \in U$, 使得 $s_2 f \equiv u + s_1 \pmod I$.

证明 蕴含关系 "(2) $\Longrightarrow$ (1)" 是显然的. 现假设叙述 (2) 不成立. 令 $T_0 = \{s_1 - f s_2 + \eta \mid s_1, s_2 \in S(W), \eta \in I\}$. 易知, T_0 满足定义 7.4.1 中条件 (1), (2) 和 (4). 如若 $-1 \in T_0$, 则 $-1 = s_1 - s_2 f + \eta$, 其中 $s_1, s_2 \in S(W)$, $\eta \in I$. 由此有, $s_2 f \equiv 1 + s_1 \pmod I$, 与假设矛盾. 从而 $-1 \notin T_0$. 因而, T_0 是环 $F[x_1, \cdots, x_n]$

的一个亚正锥. 令 $u_0 = u_1 \cdots u_r \in U$. 假若对于某个自然数 k 以及某个 $t \in T_0$, $-u_0(u_0^{2k}+t) \in T_0$, 则有 $-u_0(u_0^{2k}+s_1-s_2f+h_1) = s_3 - s_4f + h_2$, 其中 s_1, s_2, s_3, $s_4 \in S(W)$, h_1, $h_2 \in I$. 由此有 $(u_0s_2+s_4)f \equiv u_0^{2k+1}+u_0s_1+s_3 \pmod{I}$, 与假设矛盾. 因而, 对于每个自然数 n 以及每个 $t \in T_0$, $-u_0(u_0^{2k}+t) \notin T_0$. 由引理 7.4.1 知, $F[x_1,\cdots,x_n]$ 有一个亚正锥 P_1, 使得 $T_0 \subseteq P_1$, $F[x_1,\cdots,x_n] = P_1 \cup -P_1$, $P_1 \cap -P_1$ 是 $F[x_1,\cdots,x_n]$ 的一个素理想, 且 $-u_0 \notin P_1$. 令 $J = P_1 \cap -P_1$, 则 $A = F[x_1,\cdots,x_n]/J$ 是一个整环. 设 K 是 A 的分式域. 对于 $g \in F[x_1,\cdots,x_n]$, 记 $\bar{g} = g + J \in A$. 据此, 可得到 K 的如下子集:

$$Q = \{\bar{g}_1\bar{g}_2^{-1} \mid g_1,\ g_2 \in P_1,\ \text{且}\ g_2 \notin J\}.$$

容易验证, Q 是域 K 的一个正锥. 显然 $F \cap J = \{0\}$, 从而可认定 $F \subseteq K$. 此时有, $P \subseteq Q$. 设 R_1 是序域 (K,Q) 的实闭包, 则 R_1 是 F 的一个实闭扩张, 且序 $\leqslant$ 在 R_1 上的拓展恰是 R_1 的惟一序 $\leqslant_{R_1^2}$. 显然, $-f, v_1, \cdots, v_s \in T_0 \subseteq P_1$. 从而有

$$-f(\bar{x}_1,\cdots,\bar{x}_n) = \overline{-f(x_1,\cdots,x_n)} \geqslant_{R_1^2} 0,\ \text{即}\ f(\bar{x}_1,\cdots,\bar{x}_n) \leqslant_{R_1^2} 0,$$
$$v_j(\bar{x}_1,\cdots,\bar{x}_n) = \overline{v_j(x_1,\cdots,x_n)} \geqslant_{R_1^2} 0,\ j = 1, \cdots, s.$$

注意到 $u_1, \cdots, u_r \in T_0 \subseteq P_1$, 且 $u_1 \cdots u_r \notin J$. 从而有

$$u_i(\bar{x}_1,\cdots,\bar{x}_n) = \overline{u_i(x_1,\cdots,x_n)} >_{R_1^2} 0,\ i = 1, \cdots, r.$$

此外, 由熟知的 Hilbert 基定理知, 理想 I 是有限生成的. 设 $h_1, \cdots, h_t$ 是 I 的一组生成元. 由于 $I \subseteq T_0 \cap -T_0 \subseteq P_1 \cap -P_1 = J$, 从而有

$$h_k(\bar{x}_1,\cdots,\bar{x}_n) = \overline{h_k(x_1,\cdots,x_n)} = 0,\ k = 1, \cdots, t.$$

用 ϕ 表示语言 $\mathcal{L}(F,<)$ 中这样的语句: $\exists x_1 \cdots \exists x_n \phi_1 \wedge \phi_2 \wedge \phi_3 \wedge \phi_4$, 其中 ϕ_1 为 $f \leqslant 0$, ϕ_2 为 $(u_1 > 0) \wedge \cdots \wedge (u_r > 0)$, ϕ_3 为 $(v_1 \geqslant 0) \wedge \cdots \wedge (v_s \geqslant 0)$, ϕ_4 为 $(h_1 = 0) \wedge \cdots \wedge (h_t = 0)$. 由上面的关系式知, $(R_1, <_{R_1^2}) \models \phi$. 根据定理 7.3.7 知, $(R,<) \models \phi$. 从而叙述 (1) 不成立. 证毕.

由定理 7.4.2, 我们容易建立下面的结果.

定理 7.4.3(半代数非负点定理)　所设同上, 则对于 $f \in F[x_1,\cdots,x_n]$, 下列叙述等价:

(1) 对于 $a_1, \cdots, a_n \in R$, $f(a_1,\cdots,a_n) \geqslant 0$, 只要 $u_i(a_1,\cdots,a_n) > 0$, $i = 1, \cdots, r$, $v_j(a_1,\cdots,a_n) \geqslant 0$, $j = 1, \cdots, s$, 且对于每个 $h \in I$, $h(a_1,\cdots,a_n) = 0$;

(2) 存在 s_1, $s_2 \in S(W)$, $u \in U$ 以及某个非负整数 k, 使得 $(uf^{2k}+s_1)f \equiv s_2 \pmod{I}$.

证明　蕴含关系 "(2) $\Longrightarrow$ (1)" 是显然的, 下面证明蕴含关系 "(1) $\Longrightarrow$ (2)".

由叙述 (1) 知，有这样一个与其等价的叙述：对于 $a_1, \cdots, a_n \in R$，只要 $u_i(a_1,\cdots,a_n) > 0$, $i = 1, \cdots, r$, $v_j(a_1,\cdots,a_n) \geqslant 0$, $j = 1, \cdots, s$, $h(a_1,\cdots,a_n) = 0$, $\forall h \in I$, 且 $-f(a_1,\cdots,a_n) > 0$, 总有 $-1 > 0$.

令 U_1 是 $F[x_1,\cdots,x_n]$ 中由 $u_1, \cdots, u_r$ 和 $-f$ 生成的乘法么半群，而 W_1 是 $F[x_1,\cdots,x_n]$ 中由 $u_1, \cdots, u_r, v_1, \cdots, v_s$ 和 $-f$ 生成的乘法么半群. 由定理 7.4.2 知，存在 $s_1', s_2' \in S(W_1)$ 以及 $u' \in U_1$, 使得 $s_1' \cdot (-1) \equiv u' + s_2' \pmod I$. 由 $S(W_1)$ 和 U_1 中元素的形式知，$s_i' = s_{i1} - s_{i2}f$, 其中 $s_{i1}, s_{i2} \in S(W)$, $i = 1, 2$, 而 $u' = u(-f)^m$, 其中 $u \in U$, m 是一个非负整数. 从而有

$$s_{12}f - s_{11} \equiv u(-f)^m + s_{21} - s_{22}f \pmod I.$$

当 $m = 2k$ 为偶数时，由上式有 $(uf^{2k} + s_{11} + s_{21})f \equiv s_{12}f^2 + s_{22}f^2 \pmod I$. 当 $m = 2k+1$ 为奇数时，由上式有 $(uf^{2k} + s_{12} + s_{22})f \equiv s_{11} + s_{21} \pmod I$. 从而叙述 (2) 成立. 证毕.

定理 7.4.4(半代数零点定理) 所设同定理 7.4.2, 则对于 $f \in F[x_1,\cdots,x_n]$, 下列叙述等价：

(1) 对于 $a_1, \cdots, a_n \in R$, $f(a_1,\cdots,a_n) = 0$, 只要 $u_i(a_1,\cdots,a_n) > 0$, $i = 1, \cdots, r$, $v_j(a_1,\cdots,a_n) \geqslant 0$, $j = 1, \cdots, s$, 且对于每个 $h \in I$, $h(a_1,\cdots,a_n) = 0$;

(2) 有 $s \in S(W)$, $u \in U$ 以及自然数 k, 使得 $uf^{2k} + s \in I$.

证明 蕴含关系 "(2) $\Longrightarrow$ (1)" 显然成立，下面证明蕴含关系 "(1) $\Longrightarrow$ (2)".

由叙述 (1), 可推知这样一个与其等价的叙述：对于 $a_1, \cdots, a_n \in R$, 只要 $u_i(a_1,\cdots,a_n) > 0$, $i = 1, \cdots, r$, $v_j(a_1,\cdots,a_n) \geqslant 0$, $j = 1, \cdots, s$, $h(a_1,\cdots,a_n) = 0$, $\forall h \in I$, 且 $f^2(a_1,..,a_n) > 0$, 总有 $-1 > 0$.

令 U_1 是 $F[x_1,\cdots,x_n]$ 中由 $u_1, \cdots, u_r$ 和 f^2 生成的乘法么半群，W_1 是 $f[x_1,\cdots,x_n]$ 中由 $u_1, \cdots, u_r, v_1, \cdots, v_s$ 和 f^2 生成的乘法么半群，则显然 $S(W_1) = S(W)$. 由定理 7.4.2 知，存在 $s_1, s_2 \in S(W)$ 以及 $u' \in U_1$, 使得 $s_1 \cdot (-1) \equiv u' + s_2 \pmod I$. 由 U_1 中元素的形式知，$u' = uf^{2e}$, 其中 e 为非负整数. 从而有 $uf^{2(e+1)} + s_1f^2 + s_2f^2 \equiv 0 \pmod I$, 即 $uf^{2(e+1)} + s_1f^2 + s_2f^2 \in I$. 这表明叙述 (2) 成立. 证毕.

推论 1(实零点定理) 设 (F, P) 是一个实闭包为 R 的序域，I 是多项式环 $F[x_1,\cdots,x_n]$ 的一个理想，则对于 $f \in F[x_1,\cdots,x_n]$, 下列叙述等价：

(1) 对于 $a_1, \cdots, a_n \in R$, 恒有 $f(a_1,\cdots,a_n) = 0$, 只要对于每个 $h \in I$, $h(a_1,\cdots,a_n) = 0$;

(2) 有 $p_1, \cdots, p_m \in P$ 以及 $g_1, \cdots, g_m \in F[x_1,\cdots,x_n]$, 使得 $f^{2k} + \sum_{i=1}^{m} p_i g_i^2 \in I$, 其中 k 为某个自然数.

证明 在定理 7.4.4 中，取 $u_i = v_j = 1, i = 1, \cdots, r; j = 1, \cdots, s$, 即有结论. 证毕.

根据上面推论，对于域 F 的一个序 P 以及 $F[x_1, \cdots, x_n]$ 的一个理想 I, 构造 $F[x_1, \cdots, x_n]$ 的如下子集是有意义的：

$$\sqrt[R]{I} = \{f \in F[x_1, \cdots, x_n] \mid \text{有 } p_1, \cdots, p_m \in P \text{ 以及 } g_1, \cdots, g_m \in F[x_1, \cdots, x_n], \text{使得 } f^{2k} + \sum_{i=1}^{m} p_i g_i^2 \in I, \text{其中 } k \text{ 为某个自然数}\}.$$

显然，$I \subseteq \sqrt[R]{I}$. 现在证明 $\sqrt[R]{I}$ 是 $F[x_1, \cdots, x_n]$ 的一个理想. 设 $f_1, f_2 \in \sqrt[R]{I}$. 若 $a_1, \cdots, a_n \in R$, 使得对于每个 $h \in I$, $h(a_1, .., a_n) = 0$, 则由上面的推论 1 知，$f_1(a_1, \cdots, a_n) = f_2(a_1, \cdots, a_n) = 0$. 从而 $f_1(a_1, \cdots, a_n) - f_2(a_1, \cdots, a_n) = 0$. 再由上面的推论 1 知，$f_1 - f_2 \in \sqrt[R]{I}$. 同样可证，对于 $f \in \sqrt[R]{I}$ 以及 $g \in F[x_1, \cdots, x_n]$, 总有 $fg \in \sqrt[R]{I}$. 这表明 $\sqrt[R]{I}$ 为 $F[x_1, \cdots, x_n]$ 的一个理想. 理想 $\sqrt[R]{I}$ 称作 I 的实根 .

推论 2 设 (F, P) 是一个实闭包为 R 的序域，I 是 $F[x_1, \cdots, x_n]$ 的一个理想，则有 $a_1, \cdots, a_n \in R$, 使得对于每个 $h \in I$, $h(a_1, \cdots, a_n) = 0$, 当且仅当 $1 \notin \sqrt[R]{I}$.

证明 必要性显然. 现设 $1 \notin \sqrt[R]{I}$, 则由上面推论 1 知，有某些 $a_1, \cdots, a_n \in R$, 使得对于每个 $h \in I$, $h(a_1, \cdots, a_n) = 0$ (但 $1 \neq 0$). 证毕.

设 R 是一个实闭域，$\leqslant$ 是 R 的惟一序. 由 §1.2 知，R 具有由序 $\leqslant$ 所诱导的区间拓扑，它的基本开集为开区间 $]a, b[= \{x \in R \mid a < x < b\}$, 其中 $a, b \in R$, 且 $a < b$. 对于任意自然数 n, R 上 n 维线性空间 R^n 可看作 R 的 n 重乘积拓扑空间. 从而，对于所诱导的乘积区间拓扑，R^n 的基本开集具有如下形式：

$$\mathcal{O}(a_1, \cdots, a_n; \delta) := \left\{(y_1, \cdots, y_n) \in R^n \mid \sum_{i=1}^{n} (y_i - a_i)^2 < \delta^2\right\},$$

这里 δ 为 R 中的正元素，$a_i \in R, i = 1, \cdots, n$.

现在，我们将应用定理 7.3.5, 把数学分析中熟知的隐函数定理从实数域“转移”到任意实闭域上.

定理 7.4.5 设 R 是一个实闭域，$f_i(\bar{x}_j; \bar{y}_k) \in R[x_1, \cdots, x_n, y_1, .., y_m]$ 是一个 $n + m$ 元多项式，$i = 1, \cdots, m$, 且 $d(\bar{x}_j; \bar{y}_k)$ 为如下 m 级矩阵的行列式：

$$\left(\frac{\partial f_i}{\partial y_k}\right)_{m \times m},$$

其中 $\dfrac{\partial f_i}{\partial y_k}$ 表示 f_i 关于变元 y_k 的偏导数，$i, k = 1, \cdots, m$. 如果 $(\alpha; \beta) = (a_1, \cdots, a_n; b_1, \cdots, b_m) \in R^{n+m}$, 使得 $f_i(\alpha; \beta) = 0, i = 1, \cdots, m$, 且 $d(\alpha; \beta) \neq 0$, 则存在 α 在 R^n 中的一个开邻域 U 和 β 在 R^m 中的一个开邻域 V, 以及 U 到 V 的

一个连续映射 σ, 使得 $\sigma(\alpha)=\beta$, 且对于任意 $(\eta;\xi)\in U\times V$, $\sigma(\eta)=\xi$ 当且仅当 $f_i(\eta,\xi)=0$, $i=1,\cdots,m$.

证明 设诸多项式 $f_1,\cdots,f_m$ 在 R 中的全部相异系数为 $e_1,\cdots,e_r$. 相应地取新的变量 $z_1,\cdots,z_r$, 且在诸多项式 $f_1,\cdots,f_m$ 中依次将 $z_1,\cdots,z_r$ 替换 $e_1,\cdots,e_r$, 则所得的多项式 $g_1(\bar{x}_j;\bar{y}_k;\bar{z}_\ell),\cdots,g_m(\bar{x}_j;\bar{y}_k;\bar{z}_\ell)$ 是整系数多项式, 即 $g_i(\bar{x}_j;\bar{y}_k;\bar{z}_\ell)\in\mathbb{Z}[x_1,\cdots,x_n,y_1,\cdots,y_m,z_1,\cdots,z_r]$, $i=1,\cdots,m$. 令 $D(\bar{x}_j;\bar{y}_k;\bar{z}_\ell)$ 是 m 级矩阵 $\left(\dfrac{\partial g_i}{\partial y_j}\right)_{m\times m}$ 的行列式, 则 $D(\bar{x}_j;\bar{y}_k;\bar{z}_\ell)$ 是 $\mathbb{Z}$ 上一个含变量 $x_1,\cdots,x_n$, $y_1,\cdots,y_m$, $z_1,\cdots,z_r$ 的多项式.

构造序域语言中如下语句 ψ:

$$\begin{aligned}\forall z_1\cdots\forall z_r\forall x_1\cdots\forall x_n\forall y_1\cdots\forall y_m\big(&g_1=0\wedge\cdots\wedge g_m=0\wedge D\neq 0\\&\longrightarrow\exists\Delta(\Delta>0\wedge\phi_1\wedge\phi_2)\big),\end{aligned}$$

这里, ϕ_1 表示如下公式:

$$\begin{aligned}\forall u_1\cdots\forall u_n\bigg(\sum_{j=1}^{n}(u_j-x_j)^2<\Delta^2\longrightarrow\exists!v_1\cdots\exists!v_m\bigg(&\sum_{k=1}^{m}(v_k-y_k)^2<\Delta\\&\wedge g_1(\bar{u}_j;\bar{v}_k,\bar{z}_\ell)=0\wedge\cdots\wedge g_m(\bar{u}_j;\bar{v}_k;\bar{z}_\ell)=0\bigg)\bigg),\end{aligned}$$

而 ϕ_2 表示如下公式:

$$\begin{aligned}\forall u_1\cdots\forall u_n\forall v_1\cdots\forall v_m\forall\epsilon\bigg(&\sum_{j=1}^{n}(u_j-x_j)^2<\Delta^2\wedge\sum_{k=1}^{m}(v_k-y_k)^2<\Delta^2\\&\wedge g_1(\bar{u}_j;\bar{v}_k;\bar{z}_\ell)=0\wedge\cdots\wedge g_m(\bar{u}_j,;\bar{v}_k;\bar{z}_\ell)=0\wedge\epsilon>0\longrightarrow\phi_3\bigg),\end{aligned}$$

其中 ϕ_3 表示如下公式:

$$\begin{aligned}\exists\delta\bigg(\delta>0\wedge(\forall\xi_1\cdots\forall\xi_n\forall\eta_1\cdots\forall\eta_m\bigg(&\sum_{j=1}^{n}(\xi_j-x_j)^2<\Delta\wedge\sum_{k=1}^{m}(\eta_k-y_k)^2<\Delta\\&\wedge g_1(\bar{\xi}_j;\bar{\eta}_k;\bar{z}_\ell)=0\wedge\cdots\wedge g_m(\bar{\xi}_j;\bar{\eta}_k;\bar{z}_\ell)=0\\&\wedge\sum_{i=1}^{n}(\xi_i-u_i)^2<\delta\longrightarrow\sum_{j=1}^{m}(\eta_j-v_j)^2<\epsilon\bigg)\bigg).\end{aligned}$$

在上面的公式 ϕ_1 中, 符号 “$\exists!$” 意指 “惟一存在”. 显然, $\psi\in\mathrm{Sent}_0^{<}$. 根据数学分析中熟知的隐函数定理知, $(\mathbb{R},<)\models\psi$. 由定理 7.3.5 知, $(R,<)\models\psi$.

显然有

$$g_i(\bar{a}_j;\bar{b}_k;\bar{e}_\ell)=f_i(\alpha,\beta)=0,\ i=1,\cdots,m,$$

$$D(\bar{a}_j;\bar{b}_k;\bar{e}_\ell)=d(\alpha,\beta)\neq 0.$$

由表达式 $(R,<)\models\psi$ 知，有正元素 $\Delta\in R$, 使得对于任意 $\bar{u}=(u_1,\cdots,u_n)\in\mathcal{O}(a_1,\cdots,a_n;\Delta)$, 有惟一的 $\bar{v}=(v_1,\cdots,v_m)\in\mathcal{O}(b_1,\cdots,b_m;\Delta)$, 满足：$f_i(\bar{u},\bar{v})=0$, $i=1,\cdots,m$. 据此，有开邻域 $\mathcal{O}(a_1,\cdots,a_n;\Delta)$ 到 $\mathcal{O}(b_1,\cdots,b_m;\Delta)$ 的一个映射 σ, 使得 $\sigma(\bar{u})=\bar{v}$. 此时，显然有 $\sigma(\alpha)=\beta$. 此外，由公式 ϕ_2 的形式可知，映射 σ 是连续的. 证毕.

上面的定理 7.4.5 称作多项式的隐函数定理 .

第八章　高层序理论

在 E. Artin 和 O. Schreier 所创立的实域理论中，域中元素的平方和起着重要的作用. 作为 Artin-Schreier 理论的一个成功推广， E. Becker 首先在域范畴中引进了“高层亚序”和“高层序”这两个概念，并且研究了高层序 (高层亚序) 和实赋值之间的密切关系，从而建立一系列重要结论. 在高层序理论中，域中元素的高次方幂之和占有主导地位.

§8.1　Kadison-Dubois 表示定理

在本节中，我们将建立 Kadison-Dubois 表示定理，这一定理是高层序理论的一个基石. Kadison-Dubois 表示定理适合任何一个有单位元的环，这个环可以既不是结合的又不是交换的. 为简明起见，本节仅讨论有单位元的 (满足结合律的) 交换环. 因而，在本节中，所有的环均指有单位元 1 的交换环.

定义 8.1.1　环 A 的一个子集 P 称作无限亚素锥 (或简称：亚素锥), 如果下列条件成立：

(1) $0, 1 \in P$, 但 $-1 \notin P$;

(2) $P + P \subseteq P$ 且 $P \cdot P \subseteq P$.

由条件 (1) 知, 单位元 1 在加法群 $(A, +)$ 中的阶是无限的, 从而可认定：$\mathbb{Z} \subseteq A$. 此时， P 包含所有的非负整数.

定义 8.1.2　设 P 是环 A 的一个亚素维. 若对于每个 $a \in A$, 有正整数 n, 使得 $n - a \in P$, 则称 P 是 A 的一个阿基米德亚素维.

命题 8.1.1　设 P 是环 A 的一个阿基米德亚素锥，则 $A = P - P$, 即 $A = \{p_1 - p_2 \mid p_1, p_2 \in P\}$. 证毕.

证明　设 $a \in A$. 由 P 的阿基米德性知，有正整数 n, 使得 $n - a \in P$. 从而 $a = n - (n - a) \in P - P$. 因此， $A = P - P$. 证毕.

为进一步讨论，我们还需要如下定义.

定义 8.1.3　设 P 是环 A 的一个阿基米德亚素锥.　A 的一个子集 M 称作一个 P- 模，若下列条件成立：

$$0, 1 \in M,\ P \cdot M \subseteq M,\ 且\ M + M \subseteq M.$$

容易知道，对于环 A 的一个 P- 模 M, $M = A$, 当且仅当 $-1 \in M$. 事实上，若 $-1 \in M$, 则由命题 8.1.1 有， $A = P - P = P \cdot 1 + P \cdot (-1) \subseteq M + M \subseteq M$. 从而 $A = M$.

环 A 的一个 P- 模 M 称作极大的， 如果 $M \neq A$, 并且不存在 A 的 P- 模 N, 使得 $M \subset N \subset A$. 显然，对于环 A 的任意极大 P- 模 M, $-1 \notin M$.

对于环 A 的一个 P- 模 M, 其中 P 是 A 的一个阿基米德亚素锥，可构造环 A 的如下子集：

$$\mathrm{Arch}(M) = \{a \in A \mid \text{对于任意 } n \in \mathbb{N}, \text{总有 } t \in \mathbb{N}, \text{使得 } t(1+na) \in M\}.$$

对于上面子集 Arch(M), 我们有如下结论.

命题 8.1.2 所设同上，则 Arch(M) 是环 A 的一个包含 M 的 P- 模.

证明 显然，$M \subseteq \mathrm{Arch}(M)$. 设 $a, b \in \mathrm{Arch}(M)$, 则对于任意 $n \in \mathbb{N}$, 有 $s, t \in \mathbb{N}$, 使得 $s(1+2na), t(1+2nb) \in M$. 于是 $2st(1+n(a+b)) = t(s(1+2na)) + s(t(1+2nb)) \in M$. 从而 $a+b \in \mathrm{Arch}M$. 再设 $a \in \mathrm{Arch}(M)$, $p \in P$. 由于 P 是阿基米德的，从而有 $k \in \mathbb{N}$, 使得 $k-p \in P$. 此时，对于任意 $n \in \mathbb{N}$, 有 $t \in \mathbb{N}$, 使得 $t(1+kna) \in M$. 由此有

$$tk(1+npa) = p(t(1+kna)) + t(k-p) \in P \cdot M + M \subseteq M.$$

这表明： $pa \in \mathrm{Arch}(M)$. 因此， Arch(M) 是一个 P- 模. 证毕.

为了进一步刻画 Arch(M), 我们需要下面的引理.

引理 8.1.3 设 M 是环 A 的一个 P- 模，其中 P 是环 A 的一个阿基米德亚素锥. 若 $a \in A$, 但 $a \notin \mathrm{Arch}(M)$, 则存在 A 的一个极大 P- 模 S, 使得 $M \subseteq S$, 且 $-a \in S$.

证明 显然，$M - Pa$ 是环 A 的一个 P- 模. 假若 $M - Pa = A$, 则 $-1 \in M - Pa$. 从而有 $p \in P$, 使得 $pa - 1 \in M$.

考察如下由有理数组成的集合：

$$D = \left\{\frac{r}{s} \mid r, s \in \mathbb{N}, \text{使得} r + sa \in M\right\}.$$

由于 P 是阿基米德的，从而有 $n \in \mathbb{N}$, 使得 $n - (-a) \in M$, 即 $n + a \in M$. 于是， $n \in D$. 从而 D 是一个下界为 0 的非空集合.

令 d 是集合 D 的下确界，则 $d \geqslant 0$. 由于 P 是阿基米德的，从而有 $k \in \mathbb{N}$, 使得 $k - p \in P$, 且 $k > 1$. 假设 $d > 0$, 且令 $\epsilon = \min\left\{d, \dfrac{1}{k}\right\}$, 则由下确界的定义知，有 $\dfrac{r}{s} \in D$, 使得 $\dfrac{r}{s} < d + \epsilon$. 此时有

$$kr - s + ksa = (k-p)(r+sa) + s(pa-1) + rp \in M.$$

当 $kr - s > 0$ 时， $\dfrac{kr-s}{ks} \in D$. 从而 $\dfrac{kr-s}{ks} \geqslant d$. 由此有 $\dfrac{r}{s} \geqslant d + \dfrac{1}{k} \geqslant d + \epsilon$, 矛盾. 当 $kr - s < 0$ 时， $r + ksa = (kr - s + ksa) + r + (s - kr) \in M$. 从而有 $\dfrac{r}{ks} \in D$.

由此有 $\frac{r}{ks} \geqslant d$, 即 $\frac{r}{s} \geqslant kd \geqslant 2d \geqslant d + \epsilon$, 矛盾. 因而 $d = 0$.

于是, 对于任意自然数 n, 有 $\frac{r}{s} \in D$, 其中 r, $s \in \mathbb{N}$, 使得 $\frac{r}{s} < \frac{1}{n}$. 从而 $s(1+na) = n(r+sa) + (s-nr) \in M + M \subseteq M$. 这表明 $a \in \text{Arch}(M)$, 矛盾. 因而, $M - Pa \neq A$.

由 Zorn 引理可知, A 有一个极大的 P- 模 S, 使得 $M - Pa \subseteq S$. 显然, $M \subseteq S$, 且 $-a \in S$. 证毕.

现在, 我们可以建立下面的重要事实:

定理 8.1.4 设 M 是环 A 的一个 P- 模, 其中 P 是 A 的一个阿基米德亚素锥, 则

$$\text{Arch}(M) = \bigcap S,$$

这里 S 取遍 A 的所有包含 M 的极大 P- 模.

证明 设 S 是 A 的任意一个极大 P- 模, 且 $M \subseteq S$. 显然, $\text{Arch}(M) \subseteq \text{Arch}(S)$. 由命题 8.1.2 知, $\text{Arch}(S)$ 是 A 的一个 P- 模, 且 $S \subseteq \text{Arch}(S)$. 假若 $-1 \in \text{Arch}(S)$, 则有 $t \in \mathbb{N}$, 使得 $t\big(1+2\cdot(-1)\big) \in S$, 即 $-t \in S$. 从而 $-1 = (-t)+(t-1) \in S+S \subseteq S$. 此时有 $S = A$, 矛盾. 于是 $-1 \notin \text{Arch}(S)$. 由 S 的极大性知, $S = \text{Arch}(S)$, 即有 $\text{Arch}(M) \subseteq S$. 由 S 的任意性有, $\text{Arch}(M) \subseteq \bigcap S$, 这里 S 取遍 A 的所有包含 M 的极大 P- 模.

再设 $a \notin \text{Arch}(M)$, 其中 $a \in A$, 则有某个 $n \in \mathbb{N}$, 使得对于每个 $t \in \mathbb{N}$, $t(1+na) \notin M$. 此时可断言: $1+(n+1)a \notin \text{Arch}(M)$. 事实上, 如若不然, 则有某个 $s \in \mathbb{N}$, 使得 $s[1+n\big(1+(n+1)a\big)] \in M$, 从而 $s(n+1)(1+na) \in M$, 矛盾. 由引理 8.1.3 知, A 有一个极大 P- 模 S_1, 使得 $M \subseteq S_1$, 且 $-1-(n+1)a \in S_1$. 显然 $a \notin S_1$; 否则 $-1 = \big(-1-(n+1)a\big)+(n+1)a \in S_1$. 因而, $\bigcap S = \text{Arch}(M)$, 其中 S 取遍 A 的所有包含 M 的极大 P- 模. 定理获证.

命题 8.1.5 设 S 是环 A 的一个极大 P- 模, 其中 P 是 A 的一个阿基米德亚素锥, 则 $A = S \cup -S$.

证明 假若 $A \neq S \cup -S$, 则有 $a \in A$, 使得 $a \notin S \cup -S$, 即 a, $-a \notin S$. 由 S 的极大性知, $-1 \in S + Pa$, 且 $-1 \in S - Pa$. 从而有 $-1 = s_1 + p_1 a$, 且 $-1 = s_2 - p_2 a$. 其中 s_1, $s_2 \in S$, p_1, $p_2 \in P$.

于是有

$$p_1 + p_2 + s_1 p_2 + s_2 p_1 = p_1 + p_2 + (-p_1 a - 1)p_2 + (p_2 a - 1)p_1 = 0.$$

从而 $-p_1 = p_2 + s_1 p_2 + s_2 p_1 \in S$. 由命题 8.1.1 知, 元素 a 可表为: $a = p_3 - p_4$, 其中 p_3, $p_4 \in P$. 由此有 $-1 = s_1 + p_1 p_3 + (-p_1)p_4 \in S$, 矛盾. 因而, $A = S \cup -S$. 证

毕.

定义 8.1.4 设 S 是环 A 的一个 P- 模, 其中 P 是 A 的一个阿基米德亚素锥. 称 S 是 A 的一个 P- 半序, 如果 $S \neq A$, 且 $A = S \cup -S$.

根据命题 8.1.5 知, 环 A 的每个极大 P- 模都是 A 的一个 P- 半序, 如果 P 是 A 的一个阿基米德亚素锥.

定理 8.1.6 设 S 是环 A 的一个 P- 半序, 其中 P 是 A 的一个阿基米德亚素锥, 则存在惟一的 A 到实数域 $\mathbb{R}$ 的环同态 ψ, 使得 $\psi(S) \subseteq \mathbb{R}^2$. 此时有

(1) $\ker\psi = I(S)$, 这里 $I(S) := \{a \in A \mid$ 对于每个 $n \in \mathbb{N}$, $1 \pm na \in S\}$.

(2) $\psi^{-1}(\mathbb{R}^2) = S \cup I(S) = \{a \in A \mid$ 对于每个 $n \in \mathbb{N}$, $1 + na \in S\}$. 证毕.

证明 对于 $a \in A$, 有如下由有理数组成的集合:

$$D_a = \left\{\frac{r}{s} \mid r \in \mathbb{Z}, s \in \mathbb{N}, \text{且} r - sa \in S\right\}.$$

由 P 的阿基米德性可知, $D_a \neq \phi$. 此外, 有自然数 k, 使得 $k+a \in P \subseteq S$. 对于每个 $\frac{r}{s} \in D_a$, $r - sa \in S$, 其中 $r \in \mathbb{Z}$, $s \in \mathbb{N}$. 于是 $r + sk = (r - sa) + s(k+a) \in S + S \subseteq S$. 从而必有 $r + sk \geqslant 0$, 即 $\frac{r}{s} \geqslant -k$. 因而, D_a 是一个下界为 $-k$ 的非空集合. 用 $\psi(a)$ 表示 D_a 的下确界. 现在证明如下断言:

(i) 对于 $a \in A$, $\psi(-a) = -\psi(a)$;

(ii) 对于 $a, b \in A$, $\psi(a+b) = \psi(a) + \psi(b)$;

(iii) $\psi(1) = 1$;

(iv) 对于 $t \in S$, $\psi(t) \geqslant 0$;

(v) 对于 $p \in P$ 以及 $a \in A$, $\psi(ap) = \psi(a)\psi(p)$.

(i) 设 $\frac{r}{s} \in D_a$ 且 $\frac{u}{v} \in D_{-a}$, 则 $rv + us = v(r - sa) + s(u - va) \in S + S \subseteq S$. 此时必有 $rv + us \geqslant 0$, 即 $\frac{u}{v} \geqslant -\frac{r}{s}$. 由此有 $\psi(-a) \geqslant -\psi(a)$. 假若 $\psi(-a) > -\psi(a)$, 则有有理数 $\frac{m}{n}$, 其中 $m \in \mathbb{Z}$, $n \in \mathbb{N}$, 使得 $\psi(-a) > \frac{m}{n} > -\psi(a)$. 由 $\frac{m}{n} < \psi(-a)$ 知, $\frac{m}{n} \notin D_{-a}$, 即 $m + na \notin S$. 而由 $\frac{-m}{n} < \psi(a)$ 知, $\frac{-m}{n} \notin D_a$, 即 $-m - na \notin S$. 从而, $m + na \notin S \cup -S$, 矛盾. 因而 $\psi(-a) = -\psi(a)$.

(ii) 设 $\frac{r}{s} \in D_a$ 且 $\frac{u}{v} \in D_b$, 则 $(rv + us) - sv(a+b) = v(r - sa) + s(u - vb) \in S + S \subseteq S$. 从而 $\frac{rv + us}{sv} \in D_{a+b}$. 于是 $\psi(a+b) \leqslant \frac{rv+us}{sv} = \frac{r}{s} + \frac{u}{v}$. 由 $\frac{r}{s}$ 和 $\frac{u}{v}$ 的任意性知, $\psi(a+b) \leqslant \psi(a) + \psi(b)$. 由断言 (i) 又有, $\psi(a) = \psi((a+b) - b) \leqslant \psi(a+b) + \psi(-b) = \psi(a+b) - \psi(b)$. 因而 $\psi(a+b) \geqslant \psi(a) + \psi(b)$.

(iii) 注意到 $1 - 1 \cdot 1 = 0 \in S$, 即 $1 \in D_1$. 从而 $\psi(1) \leqslant 1$. 此外, 对于每个 $\frac{r}{s} \in D_1$, $r - s \in S$. 由于 $-1 \notin S$, 从而 $r - s \geqslant 0$, 即 $\frac{r}{s} \geqslant 1$. 由此知 $\psi(1) \geqslant 1$. 于是

有 $\psi(1)=1$.

(iv) 设 $t\in S$, 且 $\frac{r}{s}\in D_t$, 则 $r-st\in S$. 从而 $r=(r-st)+st\in S+S\subseteq S$. 此时必有 $r\geqslant 0$, 即 $\frac{r}{s}\geqslant 0$. 这表明 $\psi(t)\geqslant 0$.

(v) 设 $\frac{r}{s}\in D_a$, 则 $r-sa\in S$. 从而对于每个 $p\in P$, $rp-spa\in S$. 由断言 (iv) 知, $\psi(rp-spa)\geqslant 0$. 再由断言 (i) 和 (ii) 可得, $r\psi(p)-s\psi(pa)\geqslant 0$, 即 $\frac{r}{s}\psi(p)\geqslant\psi(pa)$. 由断言 (iv) 知, $\psi(p)\geqslant 0$. 从而有 $\psi(a)\psi(p)\geqslant\psi(pa)$. 由 a 的任意性知 $\psi(-a)\psi(p)\geqslant\psi(-ap)$. 由断言 (i) 知 $-\psi(a)\psi(p)\geqslant-\psi(ap)$. 从而可得 $\psi(ap)=\psi(a)\psi(p)$.

设 $a,b\in A$. 由命题 8.1.1 知, $b=p_1-p_2$, 其中 $p_1,p_2\in P$. 根据上面的断言可得 $\psi(ab)=\psi(ap_1-ap_2)=\psi(ap_1)-\psi(ap_2)=\psi(a)\big(\psi(p_1)-\psi(p_2)\big)=\psi(a)\psi(b)$. 再根据断言 (ii) 和 (iii) 知, ψ 是 A 到 R 的一个环同态. 由断言 (iv) 知, $\psi(S)\subseteq\mathbb{R}^2$.

现设 ϕ 是 A 到 $\mathbb{R}$ 的一个环同态, 使得 $\phi(S)\subseteq\mathbb{R}^2$. 对于 $a\in A$ 以及每个 $\frac{r}{s}\in D_a$, 其中 $r\in\mathbb{Z}$, $s\in\mathbb{N}$, $r-sa\in S$. 从而 $\phi(r-sa)\geqslant 0$. 由此有 $r-s\phi(a)\geqslant 0$, 即 $\phi(a)\leqslant\frac{r}{s}$. 从而 $\phi(a)\leqslant\psi(a)$, 这里 ψ 是上面所规定的环同态. 假若 $\phi(a)<\psi(a)$, 则有某个有理数 $\frac{u}{v}$, 其中 $u\in\mathbb{Z}$, $v\in\mathbb{N}$, 使得 $\phi(a)<\frac{u}{v}<\psi(a)$. 由 $\phi(a)<\frac{u}{v}$ 可知, $va-u\notin S$. 而由 $\frac{u}{v}<\psi(a)$ 可知, $u-va\notin S$. 于是 $u-va\notin S\cup -S=A$, 矛盾. 因而 $\phi(a)=\psi(a)$. 由 a 的任意性知, $\phi=\psi$. 因此, 满足上面定理中条件的环同态是惟一的.

设 $a\in\ker\psi$, 则 $\psi(a)=0$. 从而对于每个 $n\in\mathbb{N}$, $\psi(1\pm na)=\psi(1)=1\in\mathbb{R}^2$. 由此有 $1\pm na\notin -S$. 由于 $A=S\cup -S$, 从而 $1\pm na\in S$. 反过来, 设 $1\pm na\in S$, 其中 n 为任意自然数, 则 $\psi(1\pm na)\in\mathbb{R}^2$, 即 $\psi(1\pm na)\geqslant 0$. 于是有 $-\frac{1}{n}\leqslant\psi(a)\leqslant\frac{1}{n}$. 此时必有 $\psi(a)=0$, 即 $a\in\ker\psi$. 因此, 叙述 (1) 成立.

设 $a\in\psi^{-1}(\mathbb{R}^2)$, 则 $\psi(a)\geqslant 0$. 当 $\psi(a)=0$ 时, 由叙述 (1) 知, $a\in I(S)$. 当 $\psi(a)>0$ 时, 显然, $a\notin -S$. 从而 $a\in S$. 因而, $\psi^{-1}(\mathbb{R}^2)\subseteq S\cup I(S)$. 由叙述 (1) 知, 显然, $S\cup I(S)\subseteq\{a\in A\mid$ 对于每个 $n\in\mathbb{N}$, $1+na\in S\}$. 再设 $a\in A$, 使得对于每个 $n\in\mathbb{N}$, $1+na\in S$, 则 $\psi(1+na)\in\mathbb{R}^2$, 即 $\psi(1+na)\geqslant 0$. 从而 $\psi(a)\geqslant-\frac{1}{n}$. 此时必有 $\psi(a)\geqslant 0$, 即 $a\in\psi^{-1}(\mathbb{R}^2)$. 因而, $\{a\in A\mid$ 对于每个 $n\in\mathbb{N}$, $1+na\in S\}\subseteq\psi^{-1}(\mathbb{R}^2)$. 这些表明: 叙述 (2) 成立. 证毕.

现设 M 是环 A 的一个 P- 模, 其中 P 是 A 的一个阿基米德亚素锥, 且用 $\mathcal{X}(M)$ 表示由所有满足 $\psi(M)\subseteq\mathbb{R}^2$ 的环同态 ψ: $A\longrightarrow\mathbb{R}$ 组成的集合. 集合 $\mathcal{X}(M)$ 与所有包含 M 的极大 P- 模之间有着密切的联系, 这种联系可在下面的定理中看出.

定理 8.1.7 所设同上, 则在集合 $\mathcal{X}(M)$ 与 A 的所有包含 M 的极大 P- 模之

间存在如下双射：

$$\theta: \ \psi \longmapsto \psi^{-1}(\mathbb{R}^2), \quad \psi \in \mathcal{X}(M).$$

证明 首先易知，对于每个 $\psi \in \mathcal{X}(M)$, $\psi^{-1}(\mathbb{R}^2)$ 是 A 的一个包含 M 的 P- 半序. 设 S 是 A 的一个包含 $\psi^{-1}(\mathbb{R}^2)$ 的一个极大 P- 模. 由命题 8.1.5 知, S 也是 A 的 P- 半序. 根据定理 8.1.6, 有 $\phi \in \mathcal{X}(M)$, 使得 $S \subseteq \phi^{-1}(\mathbb{R}^2)$. 注意到 $\phi^{-1}(\mathbb{R}^2)$ 也是 A 的一个 P- 模. 由 S 的极大性有, $S = \phi^{-1}(\mathbb{R}^2)$. 显然, $\psi(\psi^{-1}(\mathbb{R}^2)) \subseteq \mathbb{R}^2$, 且 $\phi(\psi^{-1}(\mathbb{R}^2)) \subseteq \phi(\phi^{-1}(\mathbb{R}^2)) \subseteq \mathbb{R}^2$. 由定理 8.1.6 中惟一性知, $\phi = \psi$. 从而 $\psi^{-1}(\mathbb{R}^2) = \phi^{-1}(\mathbb{R}^2) = S$, 即 $\psi^{-1}(\mathbb{R}^2)$ 是 A 的一个包含 M 的极大 P- 模. 因此, 定理中所给的映射 θ 确是 $\mathcal{X}(M)$ 到 A 的所有包含 M 的极大 P- 模中的一个映射. 证毕.

对于 A 的任意一个包含 M 的极大 P- 模 S, 由命题 8.1.5 知, S 是 A 的一个 P- 半序. 由定理 8.1.6 知, 有 $\psi \in \mathcal{X}(M)$, 使得 $\psi(S) \subseteq \mathbb{R}^2$. 此时, $S \subseteq \psi^{-1}(\mathbb{R}^2)$. 由 S 的极大性可知, $S = \psi^{-1}(\mathbb{R}^2)$. 这表明: θ 是一个满射. 如若 $\psi^{-1}(\mathbb{R}^2) = \phi^{-1}(\mathbb{R}^2)$, 其中 $\psi, \phi \in \mathcal{X}(M)$, 则有 $\psi(\psi^{-1}(\mathbb{R}^2)) \subseteq \mathbb{R}^2$, 且 $\phi(\psi^{-1}(\mathbb{R}^2)) = \phi(\phi^{-1}(\mathbb{R}^2)) \subseteq \mathbb{R}^2$. 由定理 8.1.6 惟一性知, $\psi = \phi$. 这表明: θ 是一个单射. 证毕.

为进一步研究 $\mathcal{X}(M)$, 我们将对集合 $\mathcal{X}(M)$ 赋予一个拓扑结构. 对于 $a \in A$, 可规定 $\mathcal{X}(M)$ 到 $\mathbb{R}$ 的如下一个映射:

$$\hat{a}: \ \psi \longrightarrow \psi(a), \quad \psi \in \mathcal{X}(M).$$

于是, $\mathcal{X}(M)$ 可被赋予一个关于所有这样的映射 $\hat{a}$ $(a \in A)$ 的所谓的弱拓扑, 这个拓扑的一个子基由如下子集构成:

$$\hat{a}^{-1}(]r_1, r_2[) = \{\psi \in \mathcal{X}(M) \mid r_1 < \psi(a) < r_2\},$$

其中 $a \in A, r_1, r_2 \in \mathbb{R}$, $r_1 < r_2$, 且 $]r_1, r_2[$ 表示 $\mathbb{R}$ 中端点为 r_1 和 r_2 的开区间.

对于这样的弱拓扑, 每个映射 $\hat{a}$ 都是连续的, 其中 $a \in A$. 由亚素锥 P 的阿基米德性知, 对于每个 $a \in A$, 有自然数 n_a, 使得 $n_a \pm a \in P \subseteq M$. 从而 $\hat{a}(\mathcal{X}(M)) \subseteq [-n_a, n_a]$, 这里 $[-n_a, n_a]$ 是 $\mathbb{R}$ 中端点为 $-n_a$ 和 n_a 的闭区间. 据此, 我们可以得到拓扑空间 $\mathcal{X}(M)$ 到乘积拓扑空间 $\prod\limits_{a \in A} [-n_a, n_a]$ 的如下一个映射:

$$\pi: \ \psi \longmapsto (\psi(a))_{a \in A}, \quad \psi \in \mathcal{X}(M).$$

显然, π 是一个连续的单射. 设 $(\lambda_a)_{a \in A} \in \prod\limits_{a \in A} [-n_a, n_a]$. 若 $(\lambda_a)_{a \in A} \notin \pi(\mathcal{X}(M))$, 则有如下三种情况: (1)$\lambda_1 \neq 1$; (2) 对于某两个 $a, b \in A$, $\lambda_{a+b} \neq \lambda_a + \lambda_b$ 或 $\lambda_{ab} \neq \lambda_a \lambda_b$; (3) 对于某个 $\eta \in M$, $\lambda_\eta < 0$.

注意到, 乘积拓扑空间 $\prod\limits_{a \in A} [-n_a, n_a]$ 的一个子基由如下子集组成:

$$\mathcal{O}(d;][) = \left\{(x_a)_{a\in A} \in \prod_{a\in A}[-n_a, n_a] | x_d \in][\right\},$$

其中 $d \in A,][$ 是 $\mathbb{R}$ 中的一个开区间.

在情况 (1) 时, $(\lambda_a)_{a\in A} \in \mathcal{O}(1;]1,+\infty[)\cup\mathcal{O}(1;]-\infty,1[)$, 但 $\pi(\mathcal{X}(M))\cap(\mathcal{O}(1;]1,+\infty[)\cup\mathcal{O}(1;]-\infty,1[)) = \phi$. 在情况 (2) 时, R 中有开区间$][_1,][_2$ 和$][_3$, 使得 $\lambda_a \in][_1, \lambda_b \in][_2, \lambda_{a+b} \in][_3$ 或 $\lambda_{ab} \in][_3$, 且对于任意 $x \in][_1, y \in][_2$ 以及 $z \in][_3$, 总有 $x + y \neq z$ 或 $xy \neq z$. 令 $\mathcal{O} = \mathcal{O}(a;][_1)\cap\mathcal{O}(b;][_2)\cap\mathcal{O}(a+b;][_3)$, 或 $\mathcal{O} = \mathcal{O}(a;][_1)\cap\mathcal{O}(b;][_2)\cap\mathcal{O}(ab;][_3)$, 则 $(\lambda_a)_{a\in A} \in \mathcal{O}$, 但 $\pi(\mathcal{X}(M)) \cap \mathcal{O} = \phi$. 在情况 (3) 时, $(\lambda_a)_{a\in A} \in \mathcal{O}(\eta;]-\infty,0[)$, 但 $\pi(\mathcal{X}(M))\cap\mathcal{O}(\eta;]-\infty,0[) = \phi$. 这表明: $\pi(\mathcal{X}(M))$ 是 $\prod_{a\in A}[-n_a, n_a]$ 的一个闭子集. 根据 Tychonoff 定理知, 乘积拓扑空间 $\prod_{a\in A}[-n_a, n_a]$ 是一个 Hausdorff 紧空间, 从而 $\pi(\mathcal{X}(M))$ 是一个紧子集. 由拓扑知识, $\mathcal{X}(M)$ 同胚于 $\pi(\mathcal{X}(M))$. 因此, $\mathcal{X}(M)$ 也是一个 Hausdorff 紧空间.

记 $\mathcal{C}(\mathcal{X}(M),\mathbb{R})$ 是 $\mathcal{X}(M)$ 到 $\mathbb{R}$ 的全体连续映射组成的集合. 对于每个 $r \in \mathbb{R}$, 仍用 r 表示 $\mathcal{C}(\mathcal{X}(M),\mathbb{R})$ 中象恒为 r 的常量映射. 从而, $\mathbb{R}$ 可看作 $\mathcal{C}(\mathcal{X}(M),\mathbb{R})$ 的一个子集. 设 $f, g \in \mathcal{C}(\mathcal{X}(M),\mathbb{R})$, 且规定: $(f+g)(\psi) = f(\psi)+g(\psi)$, 且 $(fg)(\psi) = f(\psi)g(\psi)$, 其中 $\psi \in \mathcal{X}(M)$. 于是 $\mathcal{C}(\mathcal{X}(M),\mathbb{R})$ 构成一个有单位元 1 的交换环. 注意到, 对于每个 $a \in A$, $\hat{a} \in \mathcal{C}(\mathcal{X}(M),\mathbb{R})$. 从而, 我们有一个从 A 到 $\mathcal{C}(\mathcal{X}(M),\mathbb{R})$ 的环同态 Φ_M: $a \longmapsto \hat{a}$, $a \in A$.

此外, $\mathcal{C}(\mathcal{X}(M),\mathbb{R})$ 可被赋予一个拓扑, 使得它的一个基由如下子集组成:

$$\mathcal{O}(f,n) = \{g \in \mathcal{C}(\mathcal{X}(M),\mathbb{R}) \mid \text{有 } r\in\mathbb{R}, \text{使得 } r < \frac{1}{n}, \text{且对于每个 } \psi \in \mathcal{X}(M), \\ |f(\psi) - g(\psi)| < r\},$$

其中 $f \in \mathcal{C}(\mathcal{X}(M),\mathbb{R})$, $n \in \mathbb{N}$.

现在, 可以建立如下 Kadison-Dubois 表示定理.

定理 8.1.8 设 M 是环 A 的一个 P- 模, 其中 P 是 A 的一个阿基米德亚素锥, 且 $\mathrm{Arch}(M) \neq A$, 则下列结论成立:

(1) $\mathcal{X}(M)$ 是一个 Hausdorff 的紧空间;

(2) $\Phi_M^{-1}(\mathcal{C}^+(\mathcal{X}(M),\mathbb{R})) = \mathrm{Arch}(M)$, 这里 $\mathcal{C}^+(\mathcal{X}(M),\mathbb{R})$ 表示如下集合

$$\{f \in \mathcal{C}(\mathcal{X}(M),\mathbb{R}) \mid \text{对于每个} \psi \in \mathcal{X}(M),\ f(\psi) \geqslant 0\};$$

(3)$\ker\Phi_M = \{a \in A \mid \text{对于每个 } n\in\mathbb{N}, \text{有 } t\in\mathbb{N}, \text{使得 } t(1 \pm na) \in M\}$;

(4)$\mathbb{Q}\cdot\Phi_M(A)$ 在拓扑空间 $\mathcal{C}(\mathcal{X}(M),\mathbb{R})$ 中稠密.

证明 (1) 在上面讨论中, 结论 (1) 已经获证.

(2) 对于 $a \in A$, 显然 $a \in \Phi_M^{-1}(\mathcal{C}^+(\mathcal{X}(M),\mathbb{R}))$, 当且仅当对于每个 $\psi \in \mathcal{X}(M)$,

$\psi(a) \in \mathbb{R}^2$, 即 $a \in \psi^{-1}(\mathbb{R}^2)$. 由定理 8.1.7 知, $\{\psi^{-1}(\mathbb{R}^2) \mid \psi \in \mathcal{X}(M)\}$ 恰为 A 的所有包含 M 的极大 P- 模. 再由定理 8.1.4 知, 这等价于 $a \in \mathrm{Arch}(M)$. 从而结论 (2) 成立.

(3) 显然, $\ker \Phi_M = \Phi_M^{-1}\big(\mathcal{C}^+(\mathcal{X}(M),\mathbb{R})\big) \cap -\Phi_M^{-1}\big(\mathcal{C}^+(\mathcal{X}(M),\mathbb{R})\big)$. 再由结论 (2), 可推出结论 (3).

(4) 记 C 是 $\mathbb{Q}\cdot\Phi_M(A)$ 在 $\mathcal{C}(\mathcal{X}(M),\mathbb{R})$ 中的闭包. 显然, $\mathbb{R} \subseteq C$, 即 C 包含 $\mathcal{X}(M)$ 到 $\mathbb{R}$ 的全部常量映射. 由于 $\mathbb{Q}\cdot\Phi_M(A)$ 是 $\mathcal{C}(\mathcal{X}(M),\mathbb{R})$ 的子环, 从而 C 也是 $\mathcal{C}(\mathcal{X}(M),\mathbb{R})$ 的子环. 对于任意相异的 ψ, ϕ, 有某个 $a \in A$, 使得 $\psi(a) \neq \phi(a)$, 即 $\hat{a}(\psi) \neq \hat{a}(\phi)$, 其中 $\hat{a} \in \Phi_M(A) \subseteq C$. 这表明子环 C 可分离 $\mathcal{X}(M)$ 中的点. 由拓扑学中 Stone-Weierstrass 定理知, $C = \mathcal{C}(\mathcal{X}(M),\mathbb{R})$. 因此, 结论成立. 证毕.

§8.2　n 层亚序与 n 层序

在这一节中, 将在域范畴中引进 n 层亚序和 n 层序两个基本概念, 同时讨论它们的一些基本性质.

定义 8.2.1　设 F 是一个域, n 是一个自然数. 称 F 的一个子集 T 为一个 n 层亚序, 如果下列条件成立:

(1) 对于每个 $a \in F$, $a^{2n} \in T$, 即 $F^{2n} \subseteq T$;

(2) $T + T \subseteq T$, 且 $T \cdot T \subseteq T$;

(3) $-1 \notin T$.

一个 n 层亚序 T 称作完全的, 若由 $a^2 \in T$ 可推出 $a \in T \cup -T$.

显然, 域 F 的一层亚序恰是定义 1.1.4 中所说的亚正锥 (亚序). 由上面定义中条件 (3) 可知, 若域 F 有一个 n 层亚序, 则 F 的特征必为零.

对于一个域 F, 可构造 F 的如下子集:

$$\Sigma F^{2n} = \left\{ \sum_{i=1}^{m} a_i^{2n} \mid m \in \mathbb{N}, a_i \in F, i = 1, \cdots, m \right\},$$

其中 n 是自然数.

当 $-1 \notin \Sigma F^{2n}$ 时, ΣF^{2n} 显然是 F 的一个 n 层亚序, 且 ΣF^{2n} 包含在 F 的每个 n 层亚序之中. 特别地, 当 F 是一个实域时, 这些事实成立.

对于 n 层亚序, 容易建立如下事实.

命题 8.2.1　设 T 是域 F 的一个 n 层亚序, 则有

(1) $\dot{T} = T \setminus \{0\}$ 是乘法群 $\dot{F}$ 的一个子群.

(2) $T \cap -T = \{0\}$.

(3) 若 F 中元素 a 满足: $a^2 \in T$, 但 $a \notin -T$, 则 $T + Ta$ 是 F 的一个包含 T

的 n 层亚序.

证明 (1) 设 $a \in \dot{T}$, 则 $(a^{-1})^{2n} \in T$. 由 $\dot{T}$ 关于乘法的封闭性知, $a^{-1} = (a^{-1})^{2n} \cdot a^{2n-1} \in \dot{T}$. 此时可知, $\dot{T}$ 是 $\dot{F}$ 的一个子群.

(2) 显然, $0 \in T \cap -T$. 设 $a \in T \cap -T$, 则 $a, -a \in T$. 如若 $a \neq 0$, 则 $a, -a \in \dot{T}$. 由结论 (1) 知, $-1 = (-a)a^{-1} \in \dot{T} \subseteq T$, 矛盾. 因而, $T \cap -T = \{0\}$.

(3) 显然, $F^{2n} \subseteq T \subseteq T + Ta$, 且 $T + Ta$ 关于加法与乘法都是封闭的. 假若 $-1 \in T + Ta$, 则 $-1 = t_1 + t_2 a$, 其中 $t_1, t_2 \in T$. 由于 $-1 \notin T$, 从而 $t_2 \neq 0$. 由结论 (1) 知, $t_2^{-1} \in T$. 此时有 $-a = (1 + t_1)t_2^{-1} \in T$, 矛盾. 从而 $-1 \notin T + Ta$. 由定义知, $T + Ta$ 是 F 的一个 n 层亚序. 证毕.

设 T 是域 F 的一个 n 层亚序, 则由上面的命题知, $\dot{T}$ 是乘法群 $\dot{F}$ 的一个子群. 显然, 商群 $\dot{F}/\dot{T}$ 中每个元素的阶都是 $2n$ 的因子. 现设 G 是一个 Abel(乘法) 群, e 为 G 中单位元, 且 $m \in \mathbb{N}$, 使得对于所有 $g \in G$, $g^m = e$. 对于 m 的每个素因子 p, 可构造群 G 的如下子集:

$$H_p = \{g \in G \mid \text{有 } k \in \mathbb{N}, \text{使得 } g^{p^k} = e\}.$$

易见, 上面的子集 H_p 是 G 的一个子群. 该子群 H_p 称作 G 的 Sylow p - 子群. 容易证明这样一个有用的事实: 若 $p_1, \cdots, p_r$ 是 m 的所有相异的素因子, 则 G 可表为它的全部 Sylow 子群的直积

$$G = H_{p_1} \times \cdots \times H_{p_r}.$$

由此获知, 若 T 是域 F 的一个 n 层亚序, 则商群 $\dot{F}/\dot{T}$ 是它的全部 Sylow 子群的直积. 作为 n 层亚序的完全性的一个判定, 我们可建立如下结论.

命题 8.2.2 域 F 的一个 n 层亚序 Q 是完全的, 当且仅当商群 $\dot{F}/\dot{Q}$ 的 Sylow 2- 子群是循环的.

证明 对于 $a \in \dot{F}$, 用 $\bar{a}$ 表示元素 a 所在的陪集 $a\dot{Q}$, 且令 H_2 为商群 $\dot{F}/\dot{Q}$ 的 Sylow 2- 子群.

设 Q 是域 F 的一个完全的 n 层亚序. 选定 H_2 中一个元素 $\bar{a}$, 使得 $\bar{a}$ 具有最大阶. 假若 $H_2 \neq (\bar{a})$, 其中 $(\bar{a})$ 为由元 $\bar{a}$ 生成的循环子群, 则有 $\bar{b} \in H_2$, 使得 $\bar{b} \notin (\bar{a})$. 记 $(\bar{a}, \bar{b})$ 为由 $\bar{a}$ 和 $\bar{b}$ 生成的子群. 由元素 $\bar{a}$ 的选取知, 子群 $(\bar{a}, \bar{b})$ 不可能是循环的. 根据有限生成 Abel 群的结构知, $(\bar{a}, \bar{b})$ 是两个以上循环子群的直积. 从而 $(\bar{a}, \bar{b})$ 中有两个阶为 2 的相异元素 $\bar{c}$ 和 $\bar{d}$. 此时有 $c^2 \in \dot{Q}$ 且 $d^2 \in \dot{Q}$. 由 Q 的完全性知, $c, d \in -\dot{Q}$. 从而, $\bar{c} = \overline{-1} = \bar{d}$, 矛盾. 因而, $H_2 = (\bar{a})$, 即 H_2 是循环的.

反过来, 设 H_2 是循环子群. 若 $a^2 \in Q$, 其中 $a \in \dot{F}$, 则 $\bar{a}$ 是 H_2 中阶为 1 或 2 的元素. 由于循环群中阶为 1 和阶为 2 的元素都是惟一的, 从而 $\bar{a} = \bar{1}$ 或 $\bar{a} = \overline{-1}$, 即 $a \in \dot{Q} \cup -\dot{Q}$. 这表明 Q 是完全的亚序. 证毕.

设 T 是域 F 的一个 n 层亚序，则可构造 F 的如下子集：

$$\Delta(T)=\{a\in F\mid a^2\in T, \text{但 } a\notin T\cup -T\}.$$

显然，$-\Delta(T)=\Delta(T)$, 且 T 是一个完全的 n 层亚序，当且仅当 $\Delta(T)=\phi$. 由命题 8.2.1(3) 知，对于每个 $a\in\Delta(T)$, $T+Ta$ 是 F 的一个包含 T 和 a 的 n 层亚序. 实际上，我们可建立如下进一步的结果.

命题 8.2.3 设 T 是域 F 的一个不完全的 n 层亚序，则

$$T=\bigcap_{a\in\Delta(T)} T+Ta.$$

证明 由所设知，$\Delta(T)\neq\phi$. 根据命题 8.2.1(3) 知，$T\subseteq \bigcap\limits_{a\in\Delta(T)} T+Ta$. 设 $x\in \bigcap\limits_{a\in\Delta(T)} T+Ta$. 假若 $x\notin T$, 则对于每个 $a\in\Delta(T)$, $x\in(T+Ta)\cap(T-Ta)$. 从而 $x=t_1+t_2a=t_3-t_4a$, 其中 $t_1, t_2, t_3, t_4\in T$, 且 t_2 和 t_4 均不为零. 由此有 $x^2=t_1^2+t_2^2a^2+2t_1t_2a=t_3^2+t_4^2a^2-2t_3t_4a$, 从而 $t_1t_2x^2+t_3t_4x^2=t_1t_2(t_3^2+t_4^2a^2)+t_3t_4(t_1^2+t_2^2a^2)\in T$. 当 $t_1t_2+t_3t_4=0$ 时，$t_1t_2=t_3t_4=0$, 即有 $t_1=t_3=0$. 此时有，$x\in Ta\cap -Ta=(T\cap -T)a=\{0\}$, 矛盾. 当 $t_1t_2+t_3t_4\neq 0$ 时，$(t_1t_2+t_3t_4)^{-1}\in T$. 从而有 $x^2\in T$. 如若 $x\in -T$, 则 $t_4a=t_3-x\in T$. 由于 $t_4\neq 0$, 从而 $a\in T$, 矛盾于：$a\in\Delta(T)$. 于是 $x\notin -T$, 即有 $-x\in\Delta(T)$. 由此有 $x\in T-Tx$, 即 $x=t_5-t_6x$, 其中 $t_5, t_6\in T$. 注意到 $1+t_6\neq 0$, 从而 $x=(1+t_6)^{-1}t_5\in T$, 矛盾. 因此，$x\in T$. 证毕.

由命题 8.2.3, 可建立如下重要定理.

定理 8.2.4 设 T 是域 F 的一个 n 层亚序，则 $T=\bigcap Q$, 这里 Q 取遍 F 的所有包含 T 的完全 n 层亚序.

证明 只须证明：$\bigcap Q\subseteq T$, 这里 Q 取遍 F 的所有包含 T 的完全 n 层亚序. 如若不然，则有 $a\in\bigcap Q$, 但 $a\notin T$.

考察如下集合

$$\Xi=\{S\mid S \text{ 是 } F \text{ 的一个 } n \text{ 层亚序，使得 } T\subseteq S, \text{但 } a\notin S\}.$$

显然 $T\in\Xi$. 由 Zorn 引理可知，Ξ 中有一个极大元 P. 由于 a 属于 F 的每个包含 T 的完全 n 层序，从而 P 不是完全的，即 $\Delta(P)\neq\phi$. 对于每个 $b\in\Delta(P)$, 由命题 8.2.1(3) 知，$P+Pb$ 是一个真包含 P 的 n 层亚序. 由 P 的极大性知，$P+Pb\notin\Xi$, 即 $a\in P+Pb$. 此时，由命题 8.2.3 知，$a\in \bigcap\limits_{b\in\Delta(P)} P+Pb=P$, 矛盾. 因此，$\bigcap Q\subseteq T$. 证毕.

推论 1 设 T 是域 F 的一个 n 层亚序，则存在 F 的一个完全 n 层亚序 Q, 使

得 $T \subseteq Q$.

推论 2 设 F 是一个域, 且 $-1 \notin \Sigma F^{2n}$, 其中 n 为自然数, 则

(1) F 有一个完全的 n 层亚序.

(2) ΣF^{2n} 恰为 F 的所有完全的 n 层亚序的交集.

现在, 我们给出域的 n 层序的定义如下.

定义 8.2.2 域 F 的一个 n 层亚序 P 称作 n 层序, 如果乘法商群 $\dot{F}/\dot{P}$ 是一个循环群.

命题 8.2.5 设 P 是域 F 的一个 n 层序, 则

(1) $\dot{F}/\dot{P}$ 是一个阶为 $2m$ 的循环群, 其中 $m \in \mathbb{N}$, 且 $m \mid n$.

(2) P 是完全的.

证明 (1) 设 $a\dot{P}$ 是循环群 $\dot{F}/\dot{P}$ 的一个生成元, 其中 $a \in \dot{F}$, 则 $a^{2n} \in \dot{P}$, 即 $(a\dot{P})^{2n} = \dot{P}$. 因而, $\dot{F}/\dot{P}$ 是一个有限循环群, 且它的阶是 $2n$ 的一个因数. 又由于 $-\dot{P} \neq \dot{P}$, 而 $(-\dot{P})^2 = \dot{P}$, 从而 $-\dot{P}$ 是群 $\dot{F}/\dot{P}$ 中阶为 2 的元素. 这表明群 $\dot{F}/\dot{P}$ 的阶为偶数. 令 $2m$ 为群 $\dot{F}/\dot{P}$ 的阶, 其中 $m \in \mathbb{N}$, 则 $2m \mid 2n$, 即 $m \mid n$.

(2) 显然, 循环群 $\dot{F}/\dot{P}$ 的 Sylow 2 - 子群也是循环的. 由命题 8.2.2 知, P 是完全的. 证毕.

根据上面的命题 8.2.5(1), 将自然数 m 称作序 P 的恰好层, 若循环群 $\dot{F}/\dot{P}$ 的阶为 $2m$. 显然, 一层序的恰好层为 1. 此外, 由定义易知, 一个恰好层为 m 的序也可看作一个 n 层序, 只要 $m \mid n$. 更一般地, 若 T 是域 F 的一个 n 层亚序, 则 $\dot{F}/\dot{T}$ 的指数必为偶数, 因为它含有一个 2 阶元素 $-\dot{T}$. 此时, 自然数 m 称作亚序 T 的恰好层, 若商群 $\dot{F}/\dot{T}$ 的指数为 $2m$, 即 $\dot{F}/\dot{T}$中元素的最大阶为$2m$. 应该注意, 对于域 F 的一个恰好层为 m 的 n 层亚序, 仍有 $m \mid n$.

对于高层序, 我们可以建立一个类似于普通序的如下事实.

命题 8.2.6 设 P_1 和 P_2 是域 F 的恰好层相同的两个序, 且 $P_1 \subseteq P_2$, 则 $P_1 = P_2$.

证明 由所设知, $\dot{P}_2/\dot{P}_1$ 是群 $\dot{F}/\dot{P}_1$ 的子群. 由群的第一同构定理知, $\dot{F}/\dot{P}_2 \cong (\dot{F}/\dot{P}_1)/(\dot{P}_2/\dot{P}_1)$. 从而有 $|\dot{F}/\dot{P}_1| = |\dot{F}/\dot{P}_2| \cdot |\dot{P}_2/\dot{P}_1|$. 由于 $|\dot{F}/\dot{P}_1| = |\dot{F}/\dot{P}_2|$, 从而 $|\dot{P}_2/\dot{P}_1| = 1$, 即 $\dot{P}_1 = \dot{P}_2$. 因此, $P_1 = P_2$. 证毕.

由命题 8.2.5 知, 域 F 的一个 n 层序必是完全的. 不难验证, 一个完全的普通亚序 (即一层亚序) 也是一个序. 然而, 下面的例子表明: 对于高层亚序来说, 一个完全的亚序未必是一个序.

例 1 设 $F = \mathbb{Q}(x, y)$, 其中 x 和 y 是有理数域 Q 上两个未定元, 则 F 是多项式环 $\mathbb{Q}[x, y]$ 的分式域. 此外, 对所有含 x 和 y 的项规定一个字典序 $\prec$, 使得 $x \prec y$. 对于奇自然数 $n > 1$, 用 Q 表示由零元以及 F 中所有如下形式的元素组成的集合:

$$x^{kn}y^{\ell n}\frac{f(x,y)}{g(x,y)},$$

其中 $k,\ell\in\mathbb{Z}$, $f(x,y)$, $g(x,y)\in\mathbb{Q}(x,y)$, 使得积 $f(x,y)g(x,y)$ 关于字典序 $\prec$ 的尾项系数为正，且 $f(x,y)$ 和 $g(x,y)$ 都不含有因式 x 与 y.

容易验证，Q 是域 F 的一个 n 层亚序. 设 $\phi^2\in Q$, 其中 $\phi\in\dot{F}$. 显然，ϕ 可表为 $\phi=x^ry^s\dfrac{u(x,y)}{v(x,y)}$, 其中 r, $s\in\mathbb{Z}$, $u(x,y)$, $v(x,y)\in\mathbb{Q}[x,y]$, 且 $u(x,y)$ 与 $v(x,y)$ 都不含有因式 x 和 y. 于是有

$$x^{2r}y^{2s}\frac{u^2(x,y)}{v^2(x,y)}=x^{kn}y^{\ell n}\frac{f(x,y)}{g(x,y)},$$

其中 $k,\ell\in\mathbb{Z}$, $f(x,y)$, $g(x,y)\in\mathbb{Q}(x,y)$, 使得上面条件成立.

由此有 $2r=kn$, 且 $2s=\ell n$. 由于 n 为奇数，从而 k 和 ℓ 均为偶数. 令 $k=2k_1$ 且 $\ell=2\ell_1$, 则 $\phi=x^{k_1n}y^{\ell_1n}\dfrac{u(x,y)}{v(x,y)}$. 若 $u(x,y)v(x,y)$ 的尾项系数为正，则 $\phi\in Q$; 否则 $\phi\in -Q$. 因此，Q 是一个完全的 n 层亚序.

假若 Q 是 F 的一个 n 层序，则商群 $\dot{F}/\dot{Q}$ 是一个循环群，且它的阶是 $2n$ 的因数. 注意到，$(-x)^{2n}\in Q$, 但对于每个满足 $m<2n$ 的自然数 m, $(-x)^m\notin Q$. 这表明 $-x\dot{Q}$ 是群 $\dot{F}/\dot{Q}$ 中阶为 $2n$ 的元素. 从而 $-x\dot{Q}$ 必为 $\dot{F}/\dot{Q}$ 的一个生成元. 于是, $y\dot{Q}=(-x\dot{Q})^k=(-x)^k\dot{Q}$, 其中 $0\leqslant k\leqslant 2n-1$. 由此有 $(-x)^{2n-k}y\in\dot{Q}$, 这矛盾于 Q 的构造. 因此，Q 不是 F 的一个 n 层序.

现在，再给出下面的一个例子，用来表明这样一个事实：对于每个自然数 n, 确实存在恰好层为 n 的序.

例 2 设 $\widetilde{\mathbb{Q}}$ 是有理数域 $\mathbb{Q}$ 在实数域 $\mathbb{R}$ 中的实闭包，且对于 $\alpha\in\widetilde{\mathbb{Q}}$, 用 h_α 表示 α 在 $\mathbb{Q}$ 上的极小多项式.

对于每个自然数 n, 构造有理函数域 $\mathbb{Q}(x)$ 的如下子集：

$$P_{\alpha+}=\{0\}\cup\{h_\alpha^{kn}fg^{-2n}\mid k\in\mathbb{Z},\ f,\ g\in\mathbb{Q}[x],\text{使得 } g\neq 0,\text{ 而 } f(\alpha)>0\};$$

$$P_{\alpha-}=\{0\}\cup\{(-h_\alpha^{n})^kfg^{-2n}\mid k\in\mathbb{Z},\ f,\ g\in\mathbb{Q}[x],\text{使得 } g\neq 0,\text{ 而 } f(\alpha)>0\}.$$

此外，我们还可得到 $\mathbb{Q}(x)$ 的如下子集：

$$P_{+\infty}=\{0\}\cup\{x^{kn}f(x^{-1})g^{-2n}\mid k\in\mathbb{Z},\ f,\ g\in\mathbb{Q}[x],\text{使得 } g\neq 0,\text{ 而 } f(0)>0\};$$

$$P_{-\infty}=\{0\}\cup\{(-x^n)^kf(x^{-1})g^{-2n}\mid k\in\mathbb{Z},\ f,\ g\in\mathbb{Q}[x],\text{使得 } g\neq 0,\text{ 而 } f(0)>0\};$$

容易验证，上面四种形式的子集都是 $\mathbb{Q}(x)$ 的 n 层亚序. 此外，不难验证，当 n 为奇数时，上面的子集都是 $\mathbb{Q}(x)$ 的恰好层为 n 的序；而当 n 为偶数时，$P_{\alpha-}^n$ 和 $P_{-\infty}^n$ 是 $\mathbb{Q}(x)$ 的恰好层为 n 的序.

实际上，可进一步证明：有理函数域 $\mathbb{Q}(x)$ 的每个恰好层为 n 的序都可表为上面四种形式之一. 对此，可参见文献 [208].

§8.3 与 n 层序相容的赋值

在这一节中，我们将研究完全的 n 层亚序和 n 层序与赋值之间的相容性，从而建立许多重要的结论.

定义 8.3.1 设 Q 是域 F 的一个完全的 n 层亚序，v 是域 F 的一个赋值. 称 v 与 Q 相容，如果 $1+M_v \subseteq Q$, 这里 M_v 是 v 的赋值理想. 此时，亦称 A_v 与 Q 相容，这里 A_v 为 v 的赋值环.

根据命题 3.1.3 可知，定义 8.3.1 可看作定义 3.1.2 的一个推广，因为完全的一层亚序实质上是一个序.

设 Q 是域 F 的一个完全的 n 层亚序，v 是 F 的一个赋值，且 A_v, M_v 和 F_v 分别表示 v 的赋值环，赋值理想和剩余域，则可得到 F_v 的如下子集：

$$Q_v = \{\bar{a} = a + M_v \mid a \in A_v \cap Q\}.$$

容易看出，$\bar{0}, \bar{1} \in Q_v$, $Q_v + Q_v \subseteq Q_v$, $Q_v \cdot Q_v \subseteq Q_v$, 且对于每个 $\bar{a} \in F_v$, $\bar{a}^{2n} \in Q_v$.

定理 8.3.1 所设同上，且 v 与 Q 相容，则有

(1) Q_v 是 F_v 的一个完全的 n 层亚序.

(2) 如下序列是一个群同态的正合序列：

$$1 \longrightarrow \dot{F}_v/\dot{Q}_v \stackrel{\alpha}{\longrightarrow} \dot{F}/\dot{Q} \stackrel{\beta}{\longrightarrow} G_v/v(\dot{Q}) \longrightarrow 1,$$

这里 G_v 是 v 的值群，α 和 β 的规定如次：$\alpha(\bar{a}\dot{Q}_v) = a\dot{Q}$, 对于 A_v 中每个可逆元 a; $\beta(b\dot{Q}) = v(b) + v(\dot{Q})$, 对于每个非零 $b \in F$.

证明 (1) 假若 $-\bar{1} \in Q_v$, 则对于某个 $a \in A_v \cap Q$, $-\bar{1} = \bar{a}$. 从而 $1 + a = \eta$, 其中 $\eta \in M_v$. 由 v 与 Q 的相容性知，$-a = 1 - \eta \in 1 + M_v \subseteq Q$. 显然，$a \neq 0$ 且 $a^{-1} \in Q$. 于是，$-1 = a^{-1}(-a) \in Q \cdot Q \subseteq Q$, 矛盾. 因而，$-\bar{1} \notin Q_v$. 这表明 Q_v 是 F_v 的一个 n 层亚序. 设 $\bar{x}^2 \in Q_v$, 其中 $\bar{x}$ 为 F_v 中非零元，则对于某个 $a \in A_v \cap Q$, $\bar{x}^2 = \bar{a}$. 从而，$x^2 = a + \eta$, 其中 $\eta \in M_v$. 注意到 a 是 A_v 中可逆元，从而由 v 与 Q 的相容性知，$x^2 = a(1 + a^{-1}\eta) \in Q \cdot Q \subseteq Q$. 由 Q 的完全性有 $x \in Q$ 或 $x \in -Q$. 此时，$\bar{x} \in Q_v$ 或 $\bar{x} \in -Q_v$. 因此，Q_v 也是完全的.

(2) 容易验证：同态 α 和 β 的规定都是合理，α 为单射，且 β 为满射. 对于每个 $\bar{a}\dot{Q}_v \in \dot{F}_v/\dot{Q}_v$, $\beta\big(\alpha(\bar{a}\dot{Q}_v)\big) = \beta(a\dot{Q}) = v(a) + v(\dot{Q}) = v(\dot{Q})$. 从而 $\mathrm{Im}(\alpha) \subseteq \ker(\beta)$. 反过来，若 $a\dot{Q} \in \ker(\beta)$, 则 $v(a) + v(\dot{Q}) = v(\dot{Q})$, 即 $v(a) \in v(\dot{Q})$. 从而对于某

个 $t \in \dot{Q}$, $v(a) = v(t)$. 令 $b = at^{-1}$, 则 $a\dot{Q} = b\dot{Q}$, 且 b 是 A_v 中可逆元. 从而 $a\dot{Q} = \bar{b}\dot{Q} = \alpha(\bar{b}\dot{Q}_v) \in \mathrm{Im}(\alpha)$. 证毕.

下面将讨论这样一个问题：对于域 F 的一个完全的 n 层亚序 Q, F 是否有一个与 Q 相容的赋值？回答是肯定的.

设 Q 是域 F 的一个完全的 n 层亚序，则可得到 F 的如下子集：

$$A(Q) = \{a \in F \mid \text{存在自然数 } m, \text{使得 } m \pm a \in Q\};$$

$$I(Q) = \{a \in F \mid \text{对于每个自然数 } m, \frac{1}{m} \pm a \in Q\};$$

$$\mathrm{Arch}(Q) = \{a \in A(Q) \mid \text{对于每个自然数 } m, 1 + ma \in Q\}.$$

显然，$\mathbb{Q}^2 \subseteq \mathrm{Arch}(Q)$, $\mathbb{Q} \subseteq A(Q)$, 且 $\mathrm{Arch}(Q) \cap -\mathrm{Arch}(Q) = I(Q)$. 容易验证，$A(Q)$ 是域 F 的一个子环，$I(Q)$ 是 $A(Q)$ 的一个理想，且 $\mathrm{Arch}(Q)$ 具有如下性质：

$$-1 \notin \mathrm{Arch}(Q), \mathrm{Arch}(Q) + \mathrm{Arch}(Q) \subseteq \mathrm{Arch}(Q)$$
$$\text{且}\mathrm{Arch}(Q) \cdot \mathrm{Arch}(Q) \subseteq \mathrm{Arch}(Q).$$

此外，我们可建立如下结论.

命题 8.3.2 所设同上，则下列叙述成立：

(1) 若 $a \in A(Q)$, 使得对于每个 $m \in \mathbb{N}$, $1 + ma \in \mathrm{Arch}(Q)$, 则 $a \in \mathrm{Arch}(Q)$;

(2) 若 $a \in A(Q)$, 则 $a^2 \in \mathrm{Arch}(Q)$, 即对于每个 $m \in \mathbb{N}$, $1 + ma^2 \in Q$;

(3) 设 $a \in A(Q)$, 且对于某个正奇数 k, $a^k \in \mathrm{Arch}(Q)$, 则 $a \in \mathrm{Arch}(Q)$;

(4)$I(Q)$ 是环 $A(Q)$ 的一个根理想;

(5)$A(Q) = \mathrm{Arch}(Q) \cup -\mathrm{Arch}(Q)$.

证明 令 $M = Q \cap A(Q)$. 根据定义 8.1.1 和定义 8.1.2 可知，M 是环 $A(Q)$ 的一个阿基米德亚素维. 自然，M 是环 $A(Q)$ 的一个 M- 模. 注意到，对于每个 $t \in \mathbb{N}$, $\frac{1}{t} \in M$. 由此可知，$\mathrm{Arch}(M) = \mathrm{Arch}(Q)$.

(1) 由条件知, 对于每个 $m \in \mathbb{N}$, $1+m(1+(m+1)a) \in Q$, 即 $(m+1)(1+ma) \in Q$. 由于 $\dot{Q}$ 是 $\dot{F}$ 的一个乘法子群，从而 $\frac{1}{m+1} \in \dot{Q} \subseteq Q$. 于是 $1 + ma = \frac{1}{m+1}[(m+1)(1 + ma)] \in Q$. 因而 $a \in \mathrm{Arch}(Q)$.

(2) 假设对于某个 $a \in A(Q)$, $a^2 \notin \mathrm{Arch}(Q)$, 即 $a^2 \notin \mathrm{Arch}(M)$. 由定理 8.1.4 知, $A(Q)$ 有一个包含 M 的极大 M- 模 S, 使得 $a^2 \notin S$. 由定理 8.1.7 知，存在 $A(Q)$ 到实数域 $\mathbb{R}$ 的一个环同态 ψ, 使得 $\psi^{-1}(\mathbb{R}^2) \subseteq S$. 此时有，$a^2 \in \psi^{-1}(\mathbb{R}^2) \subseteq S$, 矛盾. 因而，对于每个 $a \in A(Q)$, $a^2 \in \mathrm{Arch}(Q)$.

(3) 由条件知，对于每个 $m \in \mathbb{N}$, $1 + ma^k \in Q$. 此时，显然 $1 + ma^k \in M$. 由定理 8.1.8(2) 知，$a^k \in \Phi_M^{-1}\Big(\mathcal{C}^+(\mathcal{X}(M), \mathbb{R})\Big)$. 从而，对于每个 $\psi \in \mathcal{X}(M)$, $\psi(a^k) \geqslant 0$,

即 $\psi(a)^k \geqslant 0$. 由于 k 为奇数, 从而 $\psi(a) \geqslant 0$. 这表明 $a \in \Phi_M^{-1}\Big(\mathcal{C}^+\big(\mathcal{X}(M), \mathbb{R}\big)\Big)$. 再由定理 8.1.8(2) 知, 对于每个 $m \in \mathbb{N}$, 有 $t \in \mathbb{N}$, 使得 $t(1+ma) \in M$. 由于 $M \subseteq Q$, 且 $\dfrac{1}{t} \in Q$, 从而 $1+ma \in Q$. 由 m 的任意性知, $a \in \mathrm{Arch}(Q)$.

(4) 设 $a^r \in I(Q)$, 其中 $a \in A(Q)$, $r \in \mathbb{N}$, 则对于每个 $m \in \mathbb{N}$, $\dfrac{1}{m} \pm a^r \in Q$. 由此有, $1 \pm ma^r \in M$. 由定理 8.1.8(3) 知, $a^r \in \ker(\Phi_M)$. 从而, 对于每个 $\psi \in \mathcal{X}(M)$, $\psi(a^r) = 0$, 即 $\psi(a)^r = 0$. 由此有, $a \in \ker(\Phi_M)$. 再由定理 8.1.8(3) 知, 对于每个 $m \in \mathbb{N}$, 有 $t \in \mathbb{N}$, 使得 $t(1 \pm ma) \in M$. 由此可得 $\dfrac{1}{m} \pm a \in Q$. 由 m 的任意性有, $a \in I(Q)$. 因而, $I(Q)$ 是 $A(Q)$ 的一个根理想.

(5) 设 $a \in A(Q)$. 当 $a \in Q$ 时, 显然 $a \in \mathrm{Arch}(Q) \subseteq \mathrm{Arch}(Q) \cup -\mathrm{Arch}(Q)$. 下设 $a \notin Q$. 注意到 $a^{2n} \in Q$, 从而可选取最小的自然数 k, 使得 $a^{2k} \in Q$. 由 Q 的完全性知, $a^k \in Q$ 或 $a^k \in -Q$. 当 $a^k \in Q$ 时, 由 k 的选取可知, k 必为奇数. 此时, $a^k \in Q \subseteq \mathrm{Arch}(Q)$. 由叙述 (3) 可知, $a \in \mathrm{Arch}(Q)$. 当 $a^k \in -Q$ 且 k 为奇数时, 同样有 $-a \in \mathrm{Arch}(Q)$, 即 $a \in -\mathrm{Arch}(Q)$. 当 $a^k \in -Q$ 且 k 为偶数时, $a^k \in -\mathrm{Arch}(Q)$. 此外, 由叙述 (2) 知, $a^k \in \mathrm{Arch}(Q)$. 于是, $a^k \in \mathrm{Arch}(Q) \cap -\mathrm{Arch}(Q) = I(Q)$. 根据叙述 (4) 可知, $a \in I(Q) \subseteq \mathrm{Arch}(Q)$. 证毕.

在命题 8.3.2 的基础上, 我们可以建立下面的重要定理:

定理 8.3.3 所设同命题 8.3.2, 则 $A(Q)$ 是一个与 Q 相容的实赋值环, $I(Q)$ 是 $A(Q)$ 的极大理想, 且 Q 在剩余域 $A(Q)/I(Q)$ 上所诱导的亚序 $\overline{Q}$ 是一个阿基米德正锥.

证明 首先证明 $A(Q)$ 是一个有极大理想 $I(Q)$ 的局部环. 设 $a \in A(Q) \setminus I(Q)$, 且令 $b = a^{2n}$, 则 $b \in \dot{Q}$. 由命题 8.3.2(4) 可知, $b \notin I(Q)$. 从而存在某个 $m \in \mathbb{N}$, 使得 $\dfrac{1}{m} + b \notin Q$ 或 $\dfrac{1}{m} - b \notin Q$. 注意到 $\dfrac{1}{m} + b \in Q$, 从而 $\dfrac{1}{m} - b \notin Q$. 假若 $\dfrac{1}{2m} - b \in \mathrm{Arch}(Q)$, 则 $1 + 2m(\dfrac{1}{2m} - b) \in Q$, 即 $2 - 2mb \in Q$. 由此有 $\dfrac{1}{m} - b \in Q$, 矛盾. 因而, $\dfrac{1}{2m} - b \notin \mathrm{Arch}(Q)$. 由命题 8.3.2(5) 知, $b - \dfrac{1}{2m} \in \mathrm{Arch}(Q)$. 于是 $-1 + 4mb = 1 + 4m(b - \dfrac{1}{2m}) \in Q$, 即有 $4m - b^{-1} = b^{-1}(4mb - 1) \in Q \cdot Q \subseteq Q$. 显然, $4m + b^{-1} \in Q$. 从而 $b^{-1} \in A(Q)$, 即有 $a^{-1} = a^{2n-1}b^{-1} \in A(Q)$. 这表明: $I(Q)$ 是 $A(Q)$ 的惟一极大理想, 即 $A(Q)$ 是一个极大理想为 $I(Q)$ 的局部环.

设 $a \in F$, 则 $a^{2n} \in Q$. 由于 $1 \pm \dfrac{a^{2n}}{1+a^{2n}} \in Q$, 从而 $\dfrac{a^{2n}}{1+a^{2n}} \in A(Q)$, 且 $\dfrac{1}{1+a^{2n}} = 1 - \dfrac{a^{2n}}{1+a^{2n}} \in A(Q)$. 当 $\dfrac{1}{1+a^{2n}} \notin I(Q)$ 时, $\dfrac{1}{1+a^{2n}}$ 是局部环 $A(Q)$ 中可逆元. 从而 $1+a^{2n} \in A(Q)$, 进而 $a^{2n} \in A(Q)$. 当 $\dfrac{1}{1+a^{2n}} \in I(Q)$ 时, $\dfrac{a^{2n}}{1+a^{2n}} = 1 - \dfrac{1}{1+a^{2n}} \notin I(Q)$, 即有 $\dfrac{1+a^{2n}}{a^{2n}} \in A(Q)$. 由此有 $(a^{-1})^{2n} = \dfrac{1+a^{2n}}{a^{2n}} \cdot \dfrac{1}{1+a^{2n}} \in I(Q)$.

记 B 为 $A(Q)$ 在 F 中的整闭包，则对于 $a \in F$, $a \in B$ 或 $a^{-1} \in B$. 因而，B 是 F 的一个赋值环.

假若对于某个 $b \in B$, $b^{2n} \notin A(Q)$, 则由上面的讨论知，$b^{-2n} \in I(Q)$. 记 $\mathfrak{M}$ 是 B 的极大理想，则 $b^{-2n} \in I(Q) \subseteq \mathfrak{M}$. 从而 $a^{-1} \in \mathfrak{M}$, 进而有 $1 = bb^{-1} \in \mathfrak{M}$, 矛盾. 因而，对于每个 $a \in B$, $a^{2n} \in A(Q)$, 且 $(a+k)^{2n} \in A(Q)$, $k = 1, 2, \cdots$.

借助于下面的恒等式：

$$(2n)!x = \sum_{k=0}^{2n-1} (-1)^{k+1} \binom{2n-1}{k} [(x+k)^{2n} - k^{2n}],$$

可知，对于 $a \in B$, $(2n)!a \in A(Q)$. 于是有 $a \in A(Q)$, 即有 $A(Q) = B$. 这表明 $A(Q)$ 是域 F 的一个赋值环.

对于 $\eta \in I(Q)$, 显然 $1 \pm \eta \in Q$. 根据定义 8.3.1 知，$A(Q)$ 与 Q 相容. 由定理 8.3.1 知，$\overline{Q}$ 是剩余域 $A(Q)/I(Q)$ 的一个完全的亚序. 设 $\bar{a} = a + I(Q) \in A(Q)/I(Q)$, 其中 $a \in A(Q) \setminus I(Q)$. 由命题 8.3.2 知，$a^2 \in \mathrm{Arch}(Q)$. 注意到 $a^2 \notin I(Q) = \mathrm{Arch}(Q) \cap -\mathrm{Arch}(Q)$, 从而 $a^2 \notin -\mathrm{Arch}(Q)$, 即 $-a^2 \notin \mathrm{Arch}(Q)$. 于是，有 $k \in \mathbb{N}$, 使得 $1 - ka^2 \notin Q$. 假若 $a^2 - \frac{1}{2k} \notin \mathrm{Arch}(Q)$, 则由命题 8.3.2(5) 知，$\frac{1}{2k} - a^2 \in \mathrm{Arch}(Q)$. 由此有，$2 - 2ka^2 = 1 + 2k(\frac{1}{2k} - a^2) \in Q$, 即有 $1 - ka^2 \in Q$, 矛盾. 因而 $a^2 - \frac{1}{2k} \in Arch(Q)$. 于是 $ka^2 = 1 + 2k(a^2 - \frac{1}{2k}) \in Q$, 即 $a^2 \in Q$. 从而 $\bar{a}^2 \in \overline{Q}$. 这表明 $\overline{Q}$ 是完全的一层亚序，即 $\overline{Q}$ 是域 $A(Q)/I(Q)$ 的一个普通正锥. 对于每个 $\bar{a} = a + I(Q)$, 其中 $a \in A(Q)$, 由 $A(Q)$ 的构造知，有 $m \in \mathbb{N}$, 使得 $m - a \in Q$. 从而有 $m - \bar{a} \in \overline{Q}$, 即 $\bar{a} \leqslant_{\overline{Q}} m$. 因而，$\overline{Q}$ 是 $A(Q)/I(Q)$ 的一个阿基米德正锥. 此时，$A(Q)/I(Q)$ 显然为实域，即 $A(Q)$ 是域 F 的一个实赋值环. 证毕.

由定理 8.3.3, 可推得下面的重要结果.

推论 设 F 是一个域，则下列叙述等价：

(1) 对于任意自然数 n, $-1 \notin \Sigma F^{2n}$;

(2) 对于某个自然数 m, $-1 \notin \Sigma F^{2m}$;

(3) $-1 \notin S_F$, 这里 $S_F = \Sigma F^2$;

(4) F 是一个实域.

证明 蕴含关系 "(3) $\Longrightarrow$ (4) $\Longrightarrow$ (1) $\Longrightarrow$ (2)" 是显然的，只需证明蕴含关系 "(2) $\Longrightarrow$ (3)". 设 $-1 \notin \Sigma F^{2m}$, 则 ΣF^{2m} 是域 F 的一个 m 层亚序. 由定理 8.2.4 的推论 2 知，F 有一个完全的 m 层亚序 Q. 根据定理 8.3.3, $A(Q)$ 是域 F 的一个实赋值环. 再由命题 3.1.2 的推论 2 知，$-1 \notin S_F$. 证毕.

在 §5.6 中，我们建立了重要的 Baer-Krull 定理，这一定理揭示了域的半序 (序) 和相容赋值的剩余域的半序 (序) 在构造方面的密切联系. 在下面，我们将沿着类

似的途径，探讨完全的高层亚序的结构形式. 对此，我们需要一些涉及赋值论的事实.

设 v 是域 F 的一个赋值，G_v 是 v 的值群，则 v 诱导出这样一个群的满同态 $\bar{v}$: $\dot{F}/\dot{F}^{2n} \longrightarrow G_v/2nG_v$, 使得对于 $a \in \dot{F}$, $\bar{v}(a\dot{F}^{2n}) = v(a) + 2nG_v$.

引理 8.3.4 所设同上，且 n 是自然数，则存在一个群同态 s: $G_v/2nG_v \longrightarrow \dot{F}/\dot{F}^{2n}$, 使得 $\bar{v} \circ s$ 是 $G_v/2nG_v$ 的一个恒等映射. 这样一个群同态 s 称作 $\bar{v}$ 的一个半截口.

证明 设 $2n = p_1^{k_1} \cdots p_r^{k_r}$ 是 $2n$ 的一个素因数分解，其中 $k_i > 0$, $i = 1, \cdots, r$. 借助于孙子定理 (即中国剩余定理) 可知，$G_v/2nG_v$ 到直和 $\bigoplus\limits_{i=1}^{r} G_v/p_i^{k_i}G_v$ 的如下映射是一个群同构:

$$\tau\colon\ g + 2nG_v \longmapsto (g + p_1^{k_1}G_v, \cdots, g + p_r^{k_r}G_v), \quad g \in G_v.$$

同时存在 $\dot{F}/\dot{F}^{2n}$ 到直积 $\prod\limits_{i=1}^{r} \dot{F}/\dot{F}^{p_i^{k_i}}$ 的如下同构:

$$\pi\colon\ a\dot{F}^{2n} \longmapsto (a\dot{F}^{p_1^{k_1}}, \cdots, a\dot{F}^{p_r^{k_r}}), \quad a \in \dot{F}.$$

对于任意素数 p, G_v/pG_v 可看作域 $\mathbb{Z}/(p)$ 上向量空间. 从而 G_v/pG_v 有一个基 $\{g_\lambda + pG_v \mid \lambda \in \Lambda\}$, 其中 Λ 是一个指标集. 借助于归纳法，容易证明: 对于每个 $k \in \mathbb{N}$, G_v/p^kG_v 是一个自由的 $\mathbb{Z}/(p^k)$- 模，它有一个基 $\{g_\lambda + p^kG_v \mid \lambda \in \Lambda\}$. 于是，$G_v/p^kG_v$ 中每个元素 $\bar{\gamma}$ 可惟一地表为

$$\bar{\gamma} = \Big(\sum_{\lambda \in \Lambda} m_\lambda g_\lambda\Big) + p^kG_v,$$

其中 $0 \leqslant m_\lambda < p^k$, 且除有限个外，这些 m_λ 均为零.

对于每个 $\lambda \in \Lambda$, 取定 $a_\lambda \in \dot{F}$, 使得 $v(a_\lambda) = g_\lambda$. 这样，我们可以得到 G_v/p^kG_v 到 $\dot{F}/\dot{F}^{p^k}$ 的如下映射:

$$\phi\colon\ \left(\sum_{\lambda \in \Lambda} m_\lambda g_\lambda\right) + p^kG_v \longmapsto \left(\prod_{\lambda \in \Lambda} a_\lambda^{m_\lambda}\right) \cdot \dot{F}^{p^k}.$$

显然，ϕ 是一个群同态. 记 ϕ_i: $G_v/p_i^{k_i}G_v \longrightarrow \dot{F}/\dot{F}^{p_i^{k_i}}$ 是按上面方式所获得的群同态，$i = 1, \cdots, r$. 由此可获得直和 $\bigoplus\limits_{i=1}^{r} G_v/p_i^{k_i}G_v$ 到直积 $\prod\limits_{i=1}^{r} \dot{F}/\dot{F}^{p_i^{k_i}}$ 的如下群同态:

$$\varPhi\colon\ (g + p_1^{k_1}G_v, \cdots, g + p_r^{k_r}G_v) \longmapsto \big(\phi_1(g + p_1^{k_1}G_v), \cdots, \phi_r(g + p_r^{k_r}G_v)\big), \quad g \in G_v.$$

令 $s = \pi^{-1} \circ \varPhi \circ \tau$, 则 s 为所求的群同态. 证毕.

设 $s\colon G_v/2nG_v \longrightarrow \dot{F}/\dot{F}^{2n}$ 是 $\bar{v}$ 的一个半截口，且令 $\overline{\Delta} = s(G_v/2nG_v)$，则 $\overline{\Delta}$ 是商群 $\dot{F}/\dot{F}^{2n}$ 的一个子群. 此时，可得到 $\overline{\Delta}$ 在 $\dot{F}$ 中的一个代表元集 Δ，使得 $1 \in \Delta$，且下列条件成立：

(1) 对于每个 $g \in G_v$，有惟一的 $a \in \Delta$，使得 $g + 2nG_v = v(a) + 2nG_v$；

(2) 对于 $a, b \in \Delta$，有 $c \in \Delta$，使得 $ab \in c\dot{F}^{2n}$；

(3) 对于 $a \in \Delta$，$s\big(v(a) + 2nG_v\big) = a\dot{F}^{2n}$.

事实上，有 $g \in G_v$，使得 $s(g + 2nG_v) = a\dot{F}^{2n}$. 从而有 $g + 2nG_v = \bar{v}(a\dot{F}^{2n}) = v(a) + 2nG_v$. 从而条件 (3) 成立.

再设 P_v 是 v 的剩余域 F_v 的一个普通序，G_0 是 G_v 的一个子群，$\sigma\colon G_0 \longrightarrow \{1, -1\}$ 是一个特征标，使得下列条件成立：

(1′) $2nG_v \subseteq G_0$，且 $2nG_v \subseteq \ker(\sigma)$；

(2′) 商群 G_v/G_0 的 Sylow 2- 子群是一个阶为 2^r 的循环群；

(3′) 当 $r \geqslant 1$ 时，$G_0 \cap 2^r G_v \not\subseteq \ker(\sigma)$.

记 $\overline{\Delta}_0 = s(G_0/2nG_v)$，且令 $\Delta_0 = \{a \in \Delta \mid a\dot{F}^{2n} \in \overline{\Delta}_0\}$，则 $\overline{\Delta}_0 \subseteq \overline{\Delta}$，且 Δ_0 是 $\overline{\Delta}_0$ 在 $\dot{F}$ 中的一个代表元集. 此外，可断定 $v(\Delta_0) \subseteq G_0$. 事实上，对于 $a \in \Delta_0$，$a\dot{F}^{2n} \in s(G_0/2nG_v)$. 从而，$v(a) + 2nG_v = \bar{v}(a\dot{F}^{2n}) \in G_0/2nG_v$. 因而，$v(a) \in G_0$.

对于 $a \in \Delta_0$，规定赋值环 A_v 的如下子集：

$$\Theta_a = \{z \in A_v \mid z \notin M_v, \text{且 } \sigma\big(v(a)\big)\bar{z} \in \dot{P}_v\},$$

这里 M_v 是 v 的赋值理想，$\bar{z} = z + M_v \in F_v$.

显然，对于 $a \in \Delta_0$，$\sigma\big(v(a)\big) \in \Theta_a$. 最后，我们可得到 F 的如下子集：

$$P = \bigcup_{a \in \Delta_0} a\Theta_a F^{2n}.$$

现在，我们可以建立如下面的结论.

定理 8.3.5 所设同上，则 P 是 F 的一个与 v 相容的完全 n 层亚序，且 P 在剩余域 F_v 上所诱导的亚序恰为普通序 P_v. 反过来，若 P 是 F 的一个与 v 相容的完全 n 层亚序，且 P 在 F_v 上诱导出一个普通序 P_v，则 P 可通过上面方式得到.

证明 首先，由上面的条件 (1) 可推出如下事实：对于每个 $x \in \dot{F}$，有惟一的 $a \in \Delta$，使得 $x = a\epsilon y^{2n}$，其中 $y \in \dot{F}$，$\epsilon \in A_v \setminus M_v$.

其次，还可推出如下断言：若 $a \in \Delta$，且有 $r \in \mathbb{N}$，使得 $2^r v(a) \in G_0$，则 $a^{2^r} = a_0 x^{2n}$，其中 $a_0 \in \Delta_0$，$x \in \dot{F}$.

事实上，$v(a) + G_0$ 属于 G_v/G_0 的 Sylow 2- 子群. 由于 G_v/G_0 的 Sylow 2- 子群是阶为 2^r 的循环子群，从而 $2^r v(a) \in G_0$. 由上面的条件 (2) 知，$a^{2^r} = bx^{2n}$，其中 $b \in \Delta$，$x \in \dot{F}$. 显然，$v(b) \in G_0$. 于是有 $a_0 \in \Delta_0$，使得 $v(b) + 2nG_v = v(a_0) + 2nG_v$.

此时，必有 $b = a_0 \in \Delta_0$. 因而，上面断言成立.

注意到，$\Theta_1 = \{z \in A_v \mid z \notin M_v, \text{且} \ \bar{z} \in \dot{P}_v\} \supseteq 1 + M_v$. 从而 $1 + M_v \subseteq P$, 且 $F^{2n} \subseteq P$. 此外，易知 $\overline{A_v \cap P} = \overline{\Theta}_1 \cup \{\bar{0}\} = P_v$.

设 $\alpha, \beta \in P$, 且 α 和 β 均非零，则 $\alpha = a\epsilon x^{2n}$, $\beta = b\eta y^{2n}$, 其中 $a, b \in \Delta_0$, $\epsilon \in \Theta_a$, $\eta \in \Theta_b$, 而 $x, y \in \dot{F}$. 若 $v(\alpha) \neq v(\beta)$, 不妨设 $v(\alpha) < v(\beta)$, 则 $\alpha + \beta = \alpha\epsilon' = a\epsilon\epsilon' x^{2n}$, 其中 $\epsilon' = 1 + \beta\alpha^{-1} \in 1 + M_v$. 由于 $\epsilon\epsilon' \in \Theta_a$, 从而 $\alpha + \beta \in P$. 若 $v(\alpha) = v(\beta)$, 则由上面的条件 (1) 知，$a = b$. 此时，$\alpha + \beta = ax^{2n}[\epsilon + \eta(yx^{-1})^{2n}]$, 其中 $yx^{-1} \in A_v \setminus M_v$. 由于 $\sigma(v(a))\bar{\epsilon} \in \dot{P}_v$, 且 $\sigma(v(a))\bar{\eta} = \sigma(v(b))\bar{\eta} \in \dot{P}_v$, 从而 $\bar{\eta} \in \bar{\epsilon}\dot{P}_v$. 显然，$\overline{(yx^{-1})^{2n}} \in \dot{P}_v$, 即有 $\overline{\eta(yx^{-1})^{2n}} \in \bar{\epsilon}\dot{P}_v$. 注意到陪集 $\bar{\epsilon}\dot{P}_v$ 是加法封闭的. 于是 $\overline{\epsilon + \eta(yx^{-1})^{2n}} = \bar{\epsilon} + \overline{\eta(yx^{-1})^{2n}} \in \bar{\epsilon}\dot{P}_v$, 即有 $\sigma(v(a))\overline{\epsilon + \eta(yx^{-1})^{2n}} \in \sigma(v(a))\bar{\epsilon}\dot{P}_v = P_v$. 这表明 $\epsilon + \eta(yx^{-1})^{2n} \in \Theta_a$. 因而，$\alpha + \beta \in a\Theta_a F^{2n} \subseteq P$. 此外，由上面的条件 (2) 知，$ab = cw^{2n}$, 其中 $c \in \Delta$, $w \in \dot{F}$. 由于 $s(G_0/2nG_v)$ 是 $\dot{F}/\dot{F}^{2n}$ 的一个子群，从而有

$$\begin{aligned} c\dot{F}^{2n} &= (ab)\dot{F}^{2n} = (a\dot{F}^{2n})(b\dot{F}^{2n}) \\ &\in s(G_0/2nG_v) \cdot s(G_0/2nG_v) \subseteq s(G_0/2nG_v). \end{aligned}$$

这表明 $c \in \Delta_0$. 注意到 $v(w^{2n}) \in 2nG_v \subseteq \ker(\sigma)$, 从而 $\sigma(v(c))\overline{\epsilon\eta} = \sigma(v(c) + v(w^{2n}))\overline{\epsilon\eta} = [\sigma(v(a))\bar{\epsilon}][\sigma(v(b))\bar{\eta}] \in \dot{P}_v \cdot \dot{P}_v \subseteq \dot{P}_v$, 即有 $\epsilon\eta \in \Theta_c$. 因而，$\alpha\beta = c(\epsilon\eta)(xyw)^{2n} \in c\Theta_c F^{2n} \subseteq P$. 假若 $-1 \in P$, 则 $-\bar{1} \in \overline{A_v \cap P} = P_v$, 矛盾. 因而 $-1 \notin P$. 上面论证表明：P 是域 F 的一个包含 $1 + M_v$ 的 n 层亚序，且 P 在 v 的剩余域 F_v 上诱导出正锥 P_v.

现在，需要证明 P 的完全性. 显然 $v(\dot{P}) \subseteq v(\Delta_0) + 2nG_v \subseteq G_0 + G_0 = G_0$. 设 $h \in G_0$, 则由条件 (1) 知，有 $a \in \Delta$, 使得 $h + 2nG_v = v(a) + 2nG_v$. 由条件 (3) 知，$a\dot{F}^{2n} = s(h + 2nG_v) \in s(G_0/2nG_v)$, 即有 $a \in \Delta_0$. 从而 $\sigma(v(a))a \in a\Theta_a \in \dot{P}$, 即有 $v(a) = v\Big(\sigma(v(a))a\Big) \in v(\dot{P})$. 由此有，$h \in v(a) + 2nG_v \subseteq v(\dot{P}) + v(\dot{F}^{2n}) \subseteq v(\dot{P})$. 因此，$v(\dot{P}) = G_0$. 此时可知，$v(-\dot{P}) = G_0$. 这样，我们有 $\dot{P} \cup -\dot{P} \subseteq v^{-1}(G_0)$. 设 $a \in v^{-1}(G_0)$, 则 $v(a) \in G_0 = v(\dot{P})$. 从而有 $p \in \dot{P}$, 使得 $v(a) = v(p)$. 由于 P_v 是一个普通序，且 $1 + M_v \subseteq P$, 从而可推出 $A_v \setminus M_v \subseteq \dot{P} \cup -\dot{P}$. 因而，$a = (ap^{-1})p \in (\dot{P} \cup -\dot{P}) \cdot \dot{P} = \dot{P} \cup -\dot{P}$. 因而，$v^{-1}(G_0) = \dot{P} \cup -\dot{P}$. 假若 P 不是完全的，则有 $x \in \dot{F}$, 使得 $x^2 \in \dot{P}$, 但 $x \notin \dot{P} \cup -\dot{P}$. 由上面讨论知，$2v(x) \in G_0$, 但 $v(x) \notin G_0$. 设 $w + G_0$ 是 G_v/G_0 的 Sylow 2- 子群的生成元，其中 $w \in G_v$, 则 $2^r w \in G_0$, 但 $2^{r-1}w \notin G_0$. 由于循环群中阶为 2 的元素是惟一的，从而必有 $v(x) + G_0 = 2^{r-1}w + G_0$. 令 $w = v(y)$, 其中 $y \in \dot{F}$, 则 $v(x^{-1}y^{2^{r-1}}) \in G_0$. 于是 $x^{-1}y^{2^{r-1}} \in \dot{P} \cup -\dot{P}$. 这意味着：$y^{2^{r-1}} \notin \dot{P} \cup -\dot{P}$, 而 $y^{2^r} = (x^{-1}y^{2^{r-1}})^2 x^2 \in \dot{P} \cdot \dot{P} \subseteq \dot{P}$. 由条件 (1) 知，有 $a \in \Delta$, 使得 $2^{r-1}w \in v(a) + 2nG_v$. 由此有 $y^{2^{r-1}} = a\epsilon b^{2n}$, 其中

$b\in\dot{F}$, $\epsilon\in A_v\setminus M_v$, 且进一步有 $a^2\epsilon^2b^{4n}=y^{2^r}\in\dot{P}$. 再由条件 (2) 知, $a^2=cz^{2n}$, 这里 $c\in\Delta$, $z\in\dot{F}$. 因而, $c\epsilon^2b^{2n}z^{2n}=y^{2^r}\in\dot{P}$. 注意到 $\epsilon^2\in(\dot{P}\cup-\dot{P})^2\subseteq\dot{P}$, 从而 $c\in\dot{P}$, 即有 $v(c)\in v(\dot{P})=G_0$. 于是 $c\dot{F}^{2n}=s\big(v(c)+2nG_v\big)\in s(G_0/2nG_v)$, 即有 $c\in\Delta_0$. 由 P 的规定可知, $\sigma\big(v(c)\big)\bar{\epsilon}^2\in\dot{P}_v$, 即有 $\sigma\big(v(c)\big)=1$. 进一步有 $\sigma(2^rw)=\sigma\big(v(y^{2^r})\big)=\sigma\big(v(c)\big)=1$. 显然, $2^rG_0+\langle 2^rw\rangle\subseteq G_0\cap2^rG_v$, 这里 $\langle 2^rw\rangle$ 表示由 2^rw 生成的循环子群. 另一方面, 若 $\eta\in G_0\cap2^rG_v$, 则 $\eta=2^rg$, 其中 $g\in G_v$. 注意到, $G_v/G_0=\langle w+G_0\rangle\oplus H/G_0$, 这里 H 是 G_v 的一个包含 G_0 的子群, 使得 H/G_0 是恰由 G_v/G_0 中所有阶为奇数的元素组成的子群. 从而有 $g=kw+h+g_0$, 这里 $k\in\mathbb{Z}$, $h\in H$, 且 $g_0\in G_0$. 于是 $\eta=(2^rk)w+2^rh+2^rg_0$. 由于 $2^rw\in G_0$, 从而 $2^rh\in G_0$. 令 m 为 $h+G_0$ 的阶, 则 m 为奇数, 且 $mh\in G_0$. 显然 2^r 和 m 互素, 由此可得 $h\in G_0$. 于是, $\eta=(2^rk)w+2^r(h+g_0)\in\langle 2^rw\rangle+2^rG_0$. 因而, $2^rG_0+\langle 2^rw\rangle=G_0\cap2^rG_v$. 由于 $\sigma(2^rG_0)=\{1\}$, 且 $\sigma(2^rw)=1$, 从而 $G_0\cap2^rG_v\subseteq\ker(\sigma)$, 与上面的条件 (3′) 矛盾. 因而, P 是完全的. 注意到, $1+M_v\subseteq P$. 因此, P 是 F 的一个与 v 相容的完全 n 层亚序.

现设 P 是 F 的任意一个与 v 相容的完全 n 层亚序, 使得 P 在剩余域 F_v 上诱导出一个普通序 P_v. 设 $G_0=v(\dot{P})$. 对于 $v(\alpha)\in G_0$, 其中 $\alpha\in\dot{P}$, 由条件 (1) 知, 有惟一的 $a\in\Delta$, 使得 $v(\alpha)\in v(a)+2nG_v$. 于是存在 $x\in\dot{F}$ 以及 $\epsilon\in A_v\setminus M_v$, 使得 $\alpha=a\epsilon x^{2n}$. 据此, 规定 $\sigma\big(v(\alpha)\big)=\mathrm{sgn}_{P_v}(\bar{\epsilon})$. 为证明规定的合理性, 应验证 $\sigma\big(v(\alpha)\big)$ 与 x 和 ϵ 的选取无关. 事实上, 若又有 $\alpha=a\eta y^{2n}$, 其中 $y\in\dot{F}$, $\eta\in A_v\setminus M_v$, 则 $xy^{-1}\in A_v\setminus M_v$. 从而 $\bar{\eta}\bar{\epsilon}^{-1}=\overline{xy^{-1}}^{2n}\in P_v$, 即有 $\mathrm{sgn}_{P_v}(\bar{\eta})=\mathrm{sgn}_{P_v}(\bar{\epsilon})$. 于是, 我们得到 G_0 到 $\{1,-1\}$ 的一个映射 σ. 容易验证, σ 是一个特征标. 显然, $2nG_v=v(\dot{F}^{2n})\subseteq v(\dot{P})=G_0$. 设 $\gamma=v(b)\in G_v$, 其中 $b\in\dot{F}$. 由条件 (1) 可得, $b=a\epsilon x^{2n}$, 其中 $a\in\Delta$, $x\in\dot{F}$, 且 $\epsilon\in A_v\setminus M_v$. 从而, $b^{2n}=a^{2n}\epsilon^{2n}y^{2n}$, 这里 $y=x^{2n}$. 由条件 (2) 可得, $b^{2n}=c\epsilon^{2n}z^{2n}$, 其中 $z\in\dot{F}$. 由此有 $\sigma\big(v(b^{2n})\big)=\mathrm{sgn}_{P_v}(\bar{\epsilon}^{2n})=1$, 即 $\sigma(2n\gamma)=1$. 这表明 $2nG_v\subseteq\ker(\sigma)$. 由定理 8.3.1(2) 知, G_v/G_0 是 $\dot{F}/\dot{P}$ 的同态象, 且同态核同构于 $\dot{F}_v/\dot{P}_v$, 即同态核是一个 2 阶循环群. 从而, G_v/G_0 的 Sylow 2- 子群是 $\dot{F}/\dot{P}$ 的 Sylow 2- 子群的同态象. 由命题 8.2.2 知, $\dot{F}/\dot{P}$ 的 Sylow 2- 子群是循环群, 于是 G_v/G_0 的 Sylow 2- 子群也是循环群. 令 2^r 为 G_v/G_0 的 Sylow 2- 子群的阶, 其中 $r\geqslant1$, 则有 $w\in\dot{F}$, 使得 $2^rv(w)\in G_0$, 但 $2^{r-1}v(w)\notin G_0$. 此时, 有 $\alpha\in\dot{F}$, 使得 $2^rv(w)=v(\alpha)$. 假若 $\sigma\big(v(\alpha)\big)=1$, 则 $\alpha=a\epsilon x^{2n}$, 其中 $a\in\Delta_0$, $x\in\dot{F}$, 且 $\bar{\epsilon}\in P_v$. 从而 $w^{2^r}=a(\epsilon\eta)x^{2n}$, 其中 $\eta\in A_v\setminus M_v$. 设 $w^{2^{r-1}}=b\xi y^{2n}$, 其中 $b\in\Delta$, $y\in\dot{F}$, 且 $\xi\in A_v\setminus M_v$, 则 $w^{2^r}=b^2\xi^2y^{4n}=a(\epsilon\eta)x^{2n}$. 由上面的条件 (2) 可知, $b^2\in a\dot{F}^{2n}\subseteq\dot{P}$, 即有 $w^{2^r}\in P$. 由 P 的完全性知, $w^{2^{r-1}}\in\dot{P}\cup-\dot{P}$. 由此知, $2^{r-1}v(w)=v(w^{2^{r-1}})\in v(\dot{P})=G_0$, 矛盾. 因而, $2^rv(w)=v(\alpha)\notin\ker(\sigma)$.

设 $d\in\dot{P}$, 则有 $d=b\epsilon x^{2n}$, 其中 $b\in\Delta_0$, $x\in\dot{F}$, 而 $\epsilon\in A_v\setminus M_v$. 由于

$2nG_v \subseteq \ker(\sigma)$, 从而 $\sigma(v(b)) = \sigma(v(d)) = \mathrm{sgn}_{P_v}(\bar{\epsilon})$, 即有 $\epsilon \in \Theta_b$. 由此有, $d \in b\Theta_b F^{2n} \subseteq \bigcup_{a\in\Delta_0} a\Theta_a F^{2n}$. 另一方面, 对于 $a \in \Delta_0$ 以及 $\epsilon \in \Theta_a$, $\sigma(v(a))\bar{\epsilon} \in P_v$. 由 v 和 P 的相容性知, $\sigma(v(a))\epsilon \in \dot{P}$. 由于 $v(a) \in G_0$, 从而有 $d \in \dot{P}$, 使得 $v(a) = v(d)$, 即有 $d = a\eta$, 其中 $\eta \in A_v \setminus M_v$. 由 σ 的规定知, $\sigma(v(a)) = \sigma(v(d)) = \mathrm{sgn}_{P_v}(\bar{\eta})$, 即 $\sigma(v(a))\bar{\eta} \in P_v$. 于是 $\sigma(v(a))\eta \in \dot{P}$, 即有 $\epsilon\eta^{-1} \in \dot{P}$. 因而, $a\epsilon = d(\epsilon\eta^{-1}) \in P$. 由此可得 $\bigcup_{a\in\Delta_0} a\Theta_a F^{2n} \subseteq P$. 因此, $P = \bigcup_{a\in\Delta_0} a\Theta_a F^{2n}$. 证毕.

上面定理表明这样一个事实: 对于给定的半截口 s: $G_v/2nG_v \longrightarrow \dot{F}/\dot{F}^{2n}$ 以及 $s(G_v/2nG_v)$ 在 F 中的代表元集 Δ, 所有与 v 相容的完全 n 层亚序与全体满足条件 (1′), (2′) 和 (3′) 的三要素组 (P_v, G_0, σ) 是一一对应的. 自然会问: 与 v 相容的 n 层序对应着怎样的三要素组? 对此, 我们可建立如下定理.

定理 8.3.6 所设同定理 8.3.5, P 是域 F 的一个与 v 相容的完全 n 层亚序, 且在定理 8.3.5 的意义下, (P_v, G_0, σ) 为 P 所对应的三要素组, 则 P 是域 F 的一个 n 层序, 当且仅当对于 n 的每个奇素因子 p, G_v/G_0 的 Sylow p- 子群是循环的. 此时, P 的恰好层为 $|G_v/G_0|$.

证明 由命题 8.3.1(2) 知, 我们有如下群同态的正合序列:

$$1 \longrightarrow \dot{F}_v/\dot{P}_v \xrightarrow{\ \alpha\ } \dot{F}/\dot{P} \xrightarrow{\ \beta\ } G_v/G_0 \longrightarrow 1.$$

注意到 $\dot{F}_v/\dot{P}_v$ 是一个阶为 2 的循环群, 从而 $\ker(\beta)$ 是阶为 2 的循环子群. 容易验证: 对于 n 的每个奇素因子 p, $\dot{F}/\dot{P}$ 的 Sylow p- 子群与 G_v/G_0 的 Sylow p- 子群是同构的.

若 P 是域 F 的一个 n 层序, 则 $\dot{F}/\dot{P}$ 是一个阶整除 $2n$ 的循环群. 于是, 对于 n 的每个奇素因子 p, $\dot{F}/\dot{P}$ 的 Sylow p- 子群是循环的, 即 G_v/G_0 的 Sylow p- 子群是循环的. 反过来, 若对于 n 的每个奇素因子 p, G_v/G_0 的 Sylow p- 子群是循环的, 则 $\dot{F}/\dot{P}$ 的 Sylow p- 子群也是循环的. 设 $p_1, \cdots, p_r$ 为 n 的全部相异的奇素因子, 且 H_i 为 $\dot{F}/\dot{P}$ 的 Sylow p_i- 子群, $i = 1, \cdots, r$, 则群 $\dot{F}/\dot{P}$ 可表为如下直和:

$$\dot{F}/\dot{P} = H_0 \oplus H_1 \oplus \cdots \oplus H_r,$$

这里 H_0 是 $\dot{F}/\dot{P}$ 的循环的 Sylow 2- 子群. 此时易知, $\dot{F}/\dot{P}$ 是一个循环群. 因此, P 是域 F 的一个 n 层序.

由上面的正合序列知, $|\dot{F}/\dot{P}| = 2|G_v/G_0|$, 即 P 的恰好层为 $|G_v/G_0|$. 证毕.

现在, 我们可建立下面的重要结论, 这一结论可看作定理 1.1.2 在高层亚序上的一个推广.

定理 8.3.7 设 T 是域 F 的一个 n 层亚序, 则

$$T=\bigcap P,$$

这里 P 取遍 F 的所有包含 T 的 n 层序.

证明 根据定理 8.2.4 知，只须证明：对于域 F 的一个完全的 n 层亚序 Q, $Q=\bigcap P$, 其中 P 取遍 F 的所有包含 Q 的 n 层序.

首先，我们需要证明如下关于 Abel 群的一个事实：

设 H 是一个运算为加法 "+" 的 Abel 群，$n\in\mathbb{N}$, 使得对于每个 $x\in H$, $nx=0$. 若子群族 $\mathcal{L}=\{L\mid L$ 是 H 的一个子群, 使得商群 H/L 为循环群 $\}$, 则 $\bigcap\limits_{L\in\mathcal{L}}L=\{0\}$.

为此，设 $h\in H$ 且 $h\neq 0$, 则 $h\notin\{0\}$. 由 Zorn 引理知，H 有一个子群 L_0, 它关于条件：$h\notin L_0$ 是极大的. 显然，商群 H/L_0 中每个元素的阶都是 n 的因子. 取 $\bar{g}=g+L_0\in H/L_0$, 其中 $g\in H$, 使得 $\bar{g}$ 的阶最大. 此时可断定：H/L_0 是由 $\bar{g}$ 生成的循环群. 事实上，如若不然，则有 H/L_0 中有元素 $\bar{d}$, 使得 $\bar{d}\notin\langle\bar{g}\rangle$, 这里 $\langle\bar{g}\rangle$ 表示 H/L_0 中由 $\bar{g}$ 生成的循环子群. 记 $\langle\bar{g},\bar{d}\rangle$ 是 H/L_0 中由元素 $\bar{g}$ 和 $\bar{d}$ 生成的子群. 由元素 $\bar{g}$ 的阶的最大性知，$\langle\bar{g},\bar{d}\rangle$ 不可能是循环的. 由有限生成的 Abel 群的构造知，$\langle\bar{g},\bar{d}\rangle$ 可表为它的真子群的直和形式：$\langle\bar{g},\bar{d}\rangle=V\oplus W$. 然而，根据 L_0 的极大性易知，V 和 W 都包含非单位元 $\bar{h}=h+L_0$, 矛盾. 因而，H/L_0 是一个循环群，即 $L_0\in\mathcal{L}$. 于是，$h\notin\bigcap\limits_{L\in\mathcal{L}}L$. 这表明上面事实成立.

现设 Q 是域 F 的一个完全的 n 层亚序. 由定理 8.3.3 知，$A(Q)$ 是 F 的一个与 Q 相容的赋值环. 记 v 是 $A(Q)$ 所对应的赋值，G_v 为 v 的值群，且 Q_v 是 Q 在 $A(Q)$ 的剩余域 F_v 上所诱导的阿基米德正锥. 根据定理 8.3.5 的证明知，Q 可通过满足前面的条件 $(1')$, $(2')$ 和 $(3')$ 的三要素组 (Q_v,G_0,σ) 来构造，其中 $G_0=v(\dot{Q})$, σ 是 G_0 到 $\{1,-1\}$ 的一个特征标. 将挠群 G_v/G_0 表示为直和 $G_v/G_0=H_0\oplus H$, 这里 H_0 为 G_v/G_0 的 Sylow 2- 子群，而 H 是由 G_v/G_0 中所有奇数阶元素组成的子群. 设 L 是 H 的任意一个子群，使得 H/L 为循环群. 由群同态基本定理知，G_v 有一个子群 G_0', 使得 $G_0\subseteq G_0'$, 且 $G_0'/G_0=L$. 显然，G_0'/G_0 是一个阶为奇数 m 的循环子群，从而 $mG_0'\subseteq G_0$. 据此，可规定 G_0' 到 $\{1,-1\}$ 的这样一个特征标 σ', 使得对于每个 $\eta\in G_0'$, $\sigma'(\eta)=\sigma(m\eta)$. 由于 m 为奇数，从而 $\sigma'|_{G_0}=\sigma$. 注意到，从 G_v/G_0 到 G_v/G_0' 的典型同态的核为 L, 且 L 的阶为奇数. 从而，G_v/G_0' 的 Sylow 2- 子群与 G_v/G_0 的 Sylow 2- 子群是同构的，即它们都是阶为 2^r 的循环子群. 显然 $G_0\cap 2^rG_v\subseteq G_0'\cap 2^rG_v$, 即有 $\sigma(G_0\cap 2^rG_v)=\sigma'(G_0\cap 2^rG_v)\subseteq\sigma'(G_0'\cap 2^rG_v)$. 由于 σ 满足前面的条件 $(3')$, 从而在 $r\geqslant 1$ 时，$\sigma(G_0\cap 2^rG_v)\neq\{1\}$. 此时，自然有 $\sigma'(G_0'\cap 2^rG_v)\neq\{1\}$. 这表明 (Q_v,G_0',σ') 也满足前面的条件 $(1')$, $(2')$ 和 $(3')$. 由定理 8.3.5 知，由三要素组 (Q_v,G_0',σ') 可构造出域 F 的一个完全 n 层亚序 P_L. 由于 $G_0\subseteq G_0'$ 且 $\sigma'|_{G_0}=\sigma$, 从而由定理 8.3.5 中所指明的构造方式，易知 $Q\subseteq P_L$.

易见，$G_v/G_0'\cong(G_v/G_0)/L\cong H_0\oplus H/L$. 从而，对于 n 的每个奇素因子 p,

G_v/G_0' 的 Sylow p- 子群同构于循环群 H/L 的 Sylow p- 子群. 因而, G_v/G_0' 的 Sylow p- 子群是循环的. 根据定理 8.3.6 知, P_L 是域 F 的一个 n 层序.

设子群族 $\mathcal{L} = \{L \mid L$ 是 H 的一个子群, 使得 H/L 为循环群 $\}$, 则由上面论证的事实知, $\bigcap_{L\in\mathcal{L}} L = \{0 + G_0\}$. 对于 $L \in \mathcal{L}$, 由定理 8.3.5 所指明的构造方法知, $v(\dot{P}_L)/v(\dot{Q}) = G_0'/G_0 = L$. 设 $a \in \bigcap \dot{P}$, 这里 P 取遍域 F 的所有包含 Q 的 n 层序, 则显然 $a \in \bigcap_{L\in\mathcal{L}} \dot{P}_L$. 于是, 对于每个 $L \in \mathcal{L}$, $v(a) + G_0 \in L$. 由此有 $v(a) + G_0 \in \bigcap_{L\in\mathcal{L}} L = \{0 + G_0\}$, 即 $v(a) \in G_0 = v(\dot{Q})$. 此时, $a = d\epsilon$, 其中 $d \in \dot{Q}$, $\epsilon \in A_v \setminus M_v$. 注意到 $\bar{\epsilon} \in Q_v \cup -Q_v$. 由 v 与 Q 的相容性知, $\epsilon \in Q \cup -Q$. 从而, $a = d\epsilon \in Q \cup -Q$. 假若 $a \in -Q$, 则对于 $L \in \mathcal{L}$, $-a \in P_L$, 即有 $-1 = (-a)a^{-1} \in P_L \cdot P_L \subseteq P_L$, 矛盾. 因而 $a \in Q$. 这样, $Q \supseteq \bigcap P$, 其中 P 取遍 F 的所有包含 Q 的 n 层序. 很清楚, Q 和这个交集 $\bigcap P$ 必然相等. 定理获证.

由定理 8.3.7, 定理 1.1.4 可得到如下推广.

推论 设 F 是一个实域, 则对于每个自然数 n, ΣF^{2n} 恰为 F 的所有 n 层序的交集.

§8.4 高次方幂和

从高层亚序的定义和有关结论可见, 域中元素的高次方幂和在高层序理论中是一个重要的研究对象. 在本节中, 我们将在上节的基础上, 讨论域中不同次数的方幂和之间的关系. 在本节中, 所讨论的域的特征都为零. 于是可认定, 所讨论的域都包含有理数域.

设 F 是一个域, m 为自然数, 则可构造 F 的如下子集:

$$\Sigma F^m = \left\{ \sum_{i=1}^{r} a_i^m \mid r \in \mathbb{N}, a_i \in F, i = 1, \cdots, r \right\}.$$

显然, $F^m \subseteq \Sigma F^m$, $\Sigma F^m + \Sigma F^m \subseteq \Sigma F^m$, $\Sigma F^m \cdot \Sigma F^m \subseteq \Sigma F^m$, 且 ΣF^m 中所有非零元素组成乘法群 $\dot{F}$ 的一个子群.

首先, 我们可以建立如下基本事实.

命题 8.4.1 设 F 是一个域, $m \in \mathbb{N}$, 则 $F = \Sigma F^m$, 当且仅当 m 为奇数, 或者 F 不是实域.

证明 当 m 为奇数时, 显然 $-1 \in \Sigma F^m$. 当 m 为偶数, 但 F 不是实域时, 由定理 8.3.3 的推论知, $-1 \in \Sigma F^m$. 因而, 在所给的条件下, 总有 $-1 \in \Sigma F^m$. 此时, 根据恒等式

$$m!x = \sum_{k=0}^{m-1} (-1)^{m+k} \binom{m-1}{k} [(x+k)^m - k^m]$$

可知，对于每个 $a \in F$, $m!a \in \Sigma F^m$. 注意到 $m!$ 是 ΣF^m 中非零元，从而 $a \in \Sigma F^m$. 因此， $F = \Sigma F^m$.

反过来，若 m 为偶数，且 F 是一个实域，则由定理 8.3.3 的推论知， $-1 \notin \Sigma F^m$. 因此， $F \neq \Sigma F^m$. 证毕.

由上面命题可知，值得进一步探讨的是这样的情形：域 F 为实域，且 $m = 2n$ 为偶数. 此时，根据定理 8.3.7 的推论知， ΣF^{2n} 是 F 的所有 n 层序的交集. 因而，我们有必要讨论域的高层序的存在形式.

引理 8.4.2 设 v 是域 F 的一个实赋值，且 G 为 v 的值群. 如果 $G \neq pG$, 其中 p 为素数，则对于每个 $r \in \mathbb{N}$, F 有一个恰好层为 p^r 的序.

证明 首先，设 $p = 2$. 由引理 8.3.4 的证明知，$G/2^{r+1}G$ 是一个自由的 $\mathbb{Z}/(2^{r+1})$ - 模，它有一个基 $\{g_\lambda + 2^{r+1}G \mid \lambda \in \Lambda\}$, 其中 Λ 为一个指标集. 现取定一个指标 $\lambda_0 \in \Lambda$. 由群同态基本定理知，G 有惟一的子群 G_0, 使得 $2^{r+1}G \subseteq G_0$, 且 $G_0/2^{r+1}G$ 是 $G/2^{r+1}G$ 中由元素 $2^r g_{\lambda_0} + 2^{r+1}G$ 和子集 $\{g_\lambda + 2^{r+1}G \mid \lambda \in \Lambda, 但\lambda \neq \lambda_0\}$ 所生成的子群. 显然， G/G_0 是由 $g_{\lambda_0} + G_0$ 生成的一个阶为 2^r 的循环群. 任意取定剩余域 F_v 的一个普通序 P_v. 由 $G_0/2^{r+1}G$ 的构造知，可规定 $G_0/2^{r+1}G$ 到 $\{-1, 1\}$ 的一个同态 τ, 使得 $\tau(2^r g_{\lambda_0} + 2^{r+1}G) = -1$, 而对于其他的 $\lambda \in \Lambda$, $\tau(g_\lambda + 2^{r+1}G) = 1$. 令 $\sigma = \tau \circ \pi$, 其中 π 为 G_0 到 $G_0/2^{r+1}G$ 的自然同态，则 σ 是 G_0 到 $\{1, -1\}$ 的一个特征标. 显然， $2^r g_{\lambda_0} \in G_0 \cap 2^r G$, 但 $2^r g_{\lambda_0} \notin \ker(\sigma)$. 由定理 8.3.5 和定理 8.3.6 知， F 有一个恰好层为 2^r 的序 P.

现设 $p \neq 2$. 由 $\mathbb{Z}/(p^r)$- 模 $G/p^r G$ 的自由性知， G 有一个子群 G_0, 使得 G/G_0 是一个阶为 p^r 的循环群. 此时， G/G_0 的 Sylow 2- 子群的阶为 1. 令 σ 是 G_0 到 $\{1, -1\}$ 的浅显特征标，且 P_v 为剩余域 F_v 的任意一个普通序. 由定理 8.3.5 和 8.3.6 知，三要素组 (P_v, G_0, σ) 诱导出 F 的一个恰好层为 p^r 的序. 证毕.

由上面引理，可推出下面的结论.

定理 8.4.3 设 F 是一个实域， p 是一个素数，则下列叙述等价：

(1) F 的每个实赋值的值群都是 p- 可除的；

(2) 对于每个 $n \in \mathbb{N}$, $\Sigma F^{2n} = \Sigma F^{2np}$;

(3) 对于某个 $r \in \mathbb{N}$, $\Sigma F^{2p^r} = \Sigma F^{2p^{r+1}}$;

(4) 对于某个 $m \in \mathbb{N}$, $\Sigma F^{2m} = \Sigma F^{2mp}$.

证明 蕴含关系 "(2) $\Longrightarrow$ (3) $\Longrightarrow$ (4)" 显然成立.

(1) $\Longrightarrow$ (2): 显然， $\Sigma F^{2np} \subseteq \Sigma F^{2n}$. 为证明 $\Sigma F^{2n} \subseteq \Sigma F^{2np}$, 由定理 8.2.4 的推论 2 知，只需证明 F 的每个完全的 np 层亚序也是 n 层亚序. 设 Q 是 F 的任意一

个完全的 np 层亚序. 由定理 8.3.3 知, $A(Q)$ 是 F 的一个与 Q 相容的实赋值环. 由于 $\Sigma F^{2np}\subseteq Q$, 从而由 Q 的完全性知, $\Sigma F^{np}\subseteq Q\cup -Q$. 令 v 是 $A(Q)$ 所对应的赋值, 且 $G_0=v(\dot{Q})$, 则 $npG_v=v(\dot{F}^{np})\subseteq G_0$. 由叙述 (1) 知, $G_v=pG_v$. 从而, $nG_v\subseteq G_0$. 根据定理 8.3.1(2), 我们有如下群同态的正合序列:

$$1\longrightarrow \dot{F}_v/\dot{Q}_v\longrightarrow \dot{F}/\dot{Q}\longrightarrow G_v/G_0\longrightarrow 1.$$

由此有, $\dot{F}^{2n}\subseteq \dot{Q}$, 即 $F^{2n}\subseteq Q$. 这表明: Q 也是 F 的一个完全的 n 层序.

(4) $\Longrightarrow$ (1): 令 $m=p^s t$, 其中 $s\geqslant 0$, t 为一个不被 p 整除的自然数. 假若叙述 (1) 不成立, 则 F 有一个值群为 G 的实赋值 v, 使得 $pG\neq G$. 由引理 8.4.2 知, F 有一个恰好层为 p^{s+1} 的序 P. 显然, $\Sigma F^{2mp}\subseteq \Sigma F^{2p^{s+1}}\subseteq P$. 由叙述 (4) 知, $\Sigma F^{2m}\subseteq P$, 即 P 也是一个 m 层序. 从而, p^{s+1} 整除 m, 矛盾. 因而, 叙述 (1) 成立. 证毕.

推论 1 设 F 是一个实域, 且 $m=kn$, 其中 $m,\ n,\ k\in\mathbb{N}$, 则 $\Sigma F^{2n}=\Sigma F^{2m}$, 当且仅当 F 的每个实赋值的值群是 k- 可除的.

证明 若 $\Sigma F^{2n}=\Sigma F^{2m}$, 则对于 k 的每个素因子 p, $\Sigma F^{2n}=\Sigma F^{2np}$. 由定理 8.4.3 知, F 的每个实赋值的值群都是 p- 可除的, 从而必是 k- 可除的.

反过来, 设 F 的每个实赋值的值群是 k- 可除的, 则对于 k 的每个素因子 p, 这些值群也是 p- 可除的. 令 $k=p_1p_2\cdots p_s$, 其中 $p_1,\ p_2,\ \cdots,\ p_s$ 均为素数. 重复应用定理 8.4.3 可得, $\Sigma F^{2n}=\Sigma F^{2np_1}=\Sigma F^{2np_1p_2}=\cdots=\Sigma F^{2np_1p_2\cdots p_s}=\Sigma F^{2m}$. 证毕.

推论 2 设 F 是一个实域, 则下列叙述等价:

(1) F 的每个完全的高层亚序都是普通序;

(2) F 的每个实赋值的值群都是可除的;

(3) 对于每个 $n\in\mathbb{N}$, $\Sigma F^2=\Sigma F^{2n}$.

证明 叙述 (1) 和 (3) 的等价性来自于定理 8.2.4 的推论 2(2) 以及这样一个事实: 每个完全的一层亚序即为普通序.

叙述 (2) 和 (3) 的等价性由上面的推论 1 可得. 证毕.

推论 3 若实域 F 的每个普通序都是阿基米德的, 则对于每个 $n\in\mathbb{N}$, $\Sigma F^2=\Sigma F^{2n}$.

证明 由定理 3.2.2 和命题 3.2.3 可知, F 仅具有浅显的实赋值. 由于浅显赋值的值群 $\{0\}$ 是可除的, 从而由上面的推论 2 可得结论. 证毕.

由上面的推论 3 可获得这样一个事实: 若 F 是有理数域的一个代数扩张, 则 F 中每个元素的平方都可表示为 F 中若干个元素的 $2n$ 次方幂和, 其中 n 为任意自然数.

下面的定理表明, 两个异次方幂和的同一性可以从一个域 "遗传" 到它的代数

扩域上.

定理 8.4.4 设 F 是一个域, $m, n \in \mathbb{N}$, 且 $n \mid m$. 若 $\Sigma F^{2n} = \Sigma F^{2m}$, 则对于 F 的每个代数扩张 K, $\Sigma K^{2n} = \Sigma K^{2m}$.

证明 若 K 不是实域, 则由命题 8.4.1 知, $\Sigma K^{2n} = K = \Sigma K^{2m}$. 现设 K 是一个实域, 且 w 是 K 的任意一个实赋值, 则 $v := w\mid_F$ 是域 F 的一个实赋值. 记 G_v 和 G_w 分别是 v 和 w 的值群. 由定理 8.4.3 的推论 1 知, G_v 是 k- 可除的, 其中 $k = \dfrac{m}{n}$. 由赋值论的熟知事实, 商群 G_w/G_v 中每个元素的阶都是有限的. 由此易知, G_w 也是 k- 可除的. 根据定理 8.4.3 的推论 1 知, $\Sigma K^{2n} = \Sigma K^{2m}$. 证毕.

作为一个元素可表为偶次方幂和的一个判定, 可建立下面结论.

定理 8.4.5 设 F 是一个域, $a \in \dot{F}$, 则对于自然数 n, $a \in \Sigma F^{2n}$, 当且仅当 $a \in \Sigma F^2$, 且对于 F 的每个实赋值 v, $v(a) \in 2nG_v$, 这里 G_v 是 v 的值群.

证明 设 $a \in \Sigma F^{2n}$, 则显然 $a \in \Sigma F^2$. 令 $a = \sum\limits_{i=1}^{r} b_i^{2n}$. 由命题 3.1.2 知, 对于 F 的每个实赋值 v, $v(a) = \min\{v(b_i^{2n}) \mid i = 1, \cdots r\} = \min\{2nv(b_i) \mid i = 1, \cdots, r\} \in 2nG_v$.

反过来, 设 $a \in \Sigma F^2$, 且 a 满足定理所说的其他条件. 设 Q 是域 F 的任意一个完全的 n 层亚序, 且 v 是实赋值环 $A(Q)$ 所对应的实赋值, 则由条件知, $v(a) \in 2nG_v$. 从而, $a = x^{2n}\epsilon$, 其中 $x \in \dot{F}$, ϵ 是 $A(Q)$ 中可逆元. 令 $a = \sum\limits_{i=1}^{r} b_i^2$, 则 $\epsilon = \sum\limits_{i=1}^{r}(b_i x^{-n})^2$. 此时有, $\min\{2v(b_i x^{-n}) \mid i = 1, \cdots, r\} = v(\epsilon) = 0$, 即 $b_i x^{-n} \in A(Q)$, $i = 1, \cdots, r$. 于是 $\bar{\epsilon} = \sum\limits_{i=1}^{r} \overline{b_i x^{-n}}^2 \in Q_v$. 由 v 与 Q 的相容性可知, $\epsilon \in Q$. 从而, $a \in Q$. 根据定理 8.2.4 的推论 2 知, $a \in \Sigma F^{2n}$. 证毕.

作为上面定理的一个应用, 我们可建立下面两个推论, 其中第一个推论可看作 Hilbert 第十七问题的解答在高次方幂和方面的一种推广.

推论 1 设 F 是一个实域, 且 F 在它的每个实闭包中稠密, $f \in F[x_1, \cdots, x_m]$, 这里 $F[x_1, \cdots, x_m]$ 是域 F 上 m 元多项式环, 则对于自然数 n, f 可表示为有理函数域 $F(x_1, \cdots, x_m)$ 中若干个元素的 $2n$ 次方幂之和, 当且仅当对于 F 的每个普通序 P, f 在 (F, P) 上是半正定的, 且对于 $F(x_1, \cdots, x_m)$ 的每个实赋值 v, $v(f) \in 2nG_v$, 这里 G_v 是 v 的值群.

证明 由定理 4.1.2 的推论与上面的定理 8.4.5 可得结论. 证毕.

推论 2 设 F 是一个实域, 且 F 的每个普通序都是阿基米德的. 若 $f(x)$ 是单元多项式环 $F[x]$ 中一个次数为 r 的多项式, 则对于自然数 n, $1 + f^{2n}$ 是 $F(x)$ 中若干个元素的 $2rn$ 次方幂之和.

证明 显然, $1 + f^{2n} \in \Sigma F(x)^2$. 设 v 是域 $F(x)$ 的任意一个实赋值, G 是 v

的值群，且 A 为 v 的赋值环. 由定理 3.2.2 和命题 3.2.3 知， v 在 F 上的限制是浅显的. 由命题 3.1.3 知， $G \cong \mathbb{Z}$, 且 $A=(F[x])_{p(x)}$, 其中 $p(x)$ 是 $F[x]$ 中一个不可约多项式，或者 $A=\{\frac{f}{g} \mid f, g \in F[x], g \neq 0, \text{且} \deg(f) \leqslant \deg(g)\}$. 在 $A=(F[x])_{p(x)}$ 时， $1+f^{2n}$ 是 A 中可逆元，从而 $v(1+f^{2n})=0 \in 2rnG$. 当 A 为后一种情况时， $v(1+f^{2n})=-\deg(1+f^{2n})=-2rn \in 2rnG$. 根据定理 8.4.5 知， $1+f^{2n} \in \Sigma F(x)^{2rn}$. 证毕.

此外，由定理 8.4.5, 我们还可建立下面的定理.

定理 8.4.6 设 F 是一个域, $m, n \in \mathbb{N}$, 则对于任意 $a_1, \cdots, a_r \in F$, $\left(\sum_{i=1}^{r} a_i^{2m}\right)^n \in \Sigma F^{2mn}$.

证明 令 $b=\left(\sum_{i=1}^{r} a_i^{2m}\right)^n$, 且不妨假定 $b \neq 0$, 则显然 $b \in \Sigma F^2$. 设 v 是 F 的任意实赋值，则 $v(b)=nv\left(\sum_{i=1}^{r} a_i^{2m}\right)=\min\{nv(a_i^{2m}) \mid i=1, \cdots, r\}=\min\{2mnv(a_i) \mid i=1, \cdots, r\} \in 2mnG_v$. 由定理 8.4.5 知， $b \in \Sigma F^{2mn}$. 证毕.

由上面的定理 8.4.6, 我们可以获得某种类型的恒等式，这类恒等式是首次由 D. Hilbert 提出的. 因此，这类恒等式称作 Hilbert 恒等式.

推论(Hilbert 恒等式) 设 $x_1, \cdots, x_r$ 是有理数域 $\mathbb{Q}$ 上的 r 个未定元，则对于任意 $m, n \in \mathbb{N}$, 存在如下形式的恒等式:

$$(x_1^{2m}+\cdots+x_r^{2m})^n=f_1(x_1, \cdots, x_r)^{2mn}+\cdots+f_s(x_1, \cdots, x_r)^{2mn},$$

其中 $f_i(x_1, \cdots, x_r) \in \mathbb{Q}(x_1, \cdots, x_r)$, $i=1, \cdots, s$.

§8.5 高层实闭包和高层实闭域

在本节中，我们将把普通序域的实闭包和实闭域这些概念推广到高层序中. 从研究完全亚序的拓展入手，我们将获得关于高层实闭包和高层实闭域的一些重要信息.

定义 8.5.1 设 K 是域 F 的一个扩张， P 和 Q 分别是 F 和 K 的完全亚序. 如果 $Q \cap F=P$, 且 P 和 Q 具有相同的恰好层，那么称 Q 是 P 在 K 上的一个拓展. 此时亦称 (K, Q) 是 (F, P) 的一个扩张.

显然，在上面定义中的条件下，乘法群 $\dot{F}$ 到 $\dot{K}$ 的恒等嵌入诱导出一个群同构: $\dot{F}/\dot{P} \longrightarrow \dot{K}/\dot{Q}$.

作为完全亚序的可拓展性的一个充分条件，我们可建立如下定理.

定理 8.5.1 设 P 是域 F 的一个恰好层为 n 的完全亚序， K 是 F 的一个扩

张, 且 v 是赋值环 $A(P)$ 所对应的实赋值. 如果 v 可拓展为 K 的一个赋值 w, 使得下面的两个条件成立:

(1) 商群 G_w/G_v 中每个元素的阶都是有限的, 且与 $2n$ 互素, 这里 G_v 和 G_w 分别为 v 和 w 的值群;

(2) P_v 可拓展为 w 的剩余域 K_w 的一个普通序, 这里 P_v 是 P 在 v 的剩余域 F_v 上所诱导的普通序,

那么 P 可拓展为 K 的一个完全亚序.

证明 由条件 (1) 可知, $G_w = G_v + 2nG_w$, 且 $G_v \cap 2nG_w = 2nG_v$. 从而 G_v 到 G_w 的恒等嵌入诱导出一个群同构 τ: $G_v/2nG_v \longrightarrow G_w/2nG_w$. 令 $G_0 = v(\dot{P})$, 则 $2nG_v \subseteq G_0$. 于是, τ 诱导出群同构 π: $G_v/G_0 \longrightarrow G_w/G_0 + 2nG_w$.

设 s_v: $G_v/2nG_v \longrightarrow \dot{F}/\dot{F}^{2n}$ 是 $\bar{v}$ 的一个半截口, 且令 s_w 为 τ^{-1} 和 s_v 的合成映射, 则 s_w: $G_w/2nG_w \longrightarrow \dot{F}/\dot{F}^{2n}$ 是 $\bar{w}$ 的一个半截口. 取定 $s_v(G_v/2nG_v)$ 在 $\dot{F}$ 中一个代表元集 Δ, 则 Δ 也是 $s_w(G_w/2nG_w)$ 在 $\dot{K}$ 中一个代表元集. 令 $G_0' = G_0 + 2nG_w$, 则 $s_v(G_0/2nG_v)$ 和 $s_w(G_0'/2nG_w)$ 在 Δ 中的代表元子集相同, 且记作 Δ_0. 设 σ: $G_0 \longrightarrow \{1,-1\}$ 是由 P 所确定的特征标, 则可规定 G_0' 到 $\{1,-1\}$ 的这样一个特征标 σ', 使得对于每个 $g_0 \in G_0$ 以及 $\eta \in G_w$, $\sigma'(g_0 + 2n\eta) = \sigma(g_0)$. 由同构 π 知, G_w/G_0' 和 G_v/G_0 的 Sylow 2- 子群同构, 从而它们都是阶为 2^r 的循环子群. 由条件 (2) 知, P_v 在 K_w 上可拓展为一个普通序 Q_w. 由包含关系 $G_0 \cap 2^rG_v \subseteq G_0' \cap 2^rG_w$ 可知, 三要素组 (Q_w, G_0', σ') 满足定理 8.3.5 中所要求的条件. 由定理 8.3.5 知, 这个三要素组确定域 K 的一个完全的 n 层亚序 Q, 使得 $Q = \bigcup\limits_{a \in \Delta_0} a\Theta_a K^{2n}$, 这里 Θ_a 的规定同定理 8.3.5 中所示.

设 $b \in \dot{P}$, 则 $v(b) \in G_0$. 从而 $v(b) \in v(a) + 2nG_v$, 其中 $a \in \Delta_0$. 由此有 $b = a\epsilon x^{2n}$, 其中 $x \in \dot{F}$, $\epsilon \in A_v \setminus M_v \subseteq A_w \setminus M_w$. 注意到, P 是由三要素组 (P_v, G_0, σ) 所确定的. 从而 $\sigma(v(a))\bar{\epsilon} \in P_v$, 即有 $\sigma'(w(a))\bar{\epsilon} \in Q_w$. 这表明 $\epsilon \in \Theta_a$, 从而 $b \in a\Theta_a K^{2n} \subseteq Q$. 因而, $P \subseteq Q \cap F$. 反过来, 设 $b \in \dot{Q} \cap F$, 则 $b = azy^{2n}$, 其中 $a \in \Delta_0$, $z \in \Theta_a$, $y \in \dot{K}$. 由此知, $2nw(y) = w(b) - w(a) = v(b) - v(a) \in G_v$. 由条件 (1) 知, $w(y) \in G_v$, 即对于某个 $x \in \dot{F}$, $w(y) = v(x)$. 于是 $b = a\epsilon x^{2n}$, 其中 $\epsilon = z(yx^{-1})^{2n} \in A_v \setminus M_v$. 此时, $\sigma(v(a))\bar{\epsilon} = \sigma'(w(a))\bar{z}(\overline{yx^{-1}})^{2n} \in Q_w$, 即有 $\sigma(v(a))\bar{\epsilon} \in Q_w \cap F_v = P_v$. 由 P 与三要素组 (P_v, G_0, σ) 的对应关系知, $b = a\epsilon x^{2n} \in P$. 因而, $Q \cap F \subseteq P$, 即有 $Q \cap F = P$. 此外, Q 的恰好层为: $|G_w/G_0'| = |G_v/G_0| = n$. 因此, Q 是 P 在 K 上的一个拓展. 证毕.

由于赋值域的 Hensel 化是一个直接扩张, 从而由定理 8.5.1 可得到如下结果:

推论 设 P 是域 F 的一个完全的 n 层亚序, v 是由赋值环 $A(P)$ 所确定的实赋值, 则 P 可拓展为 F 关于 v 的 Hensel 化的一个完全的 n 层亚序.

定义 8.5.2 设 P 是域 F 的一个完全的 n 层亚序, (R, Q) 是 (F, P) 的一个扩

张. 如果 R 是 F 的代数扩张, 且 Q 在 R 的每个真代数扩张上不能再拓展, 那么称 (R,Q) 是 (F,P) 的一个实闭包.

类似于证明普通序域的极大序扩张的存在性 (见定理 1.3.5 的证明), 可以证明: 对于域 F 的每个完全亚序 P, (F,P) 都有一个实闭包.

对于高层亚序的实闭包, 我们可以建立下面的基本结论.

定理 8.5.2 设 P 是域 F 的一个完全的 n 层亚序, (R,Q) 是 (F,P) 的一个实闭包, 则 $A(Q)$ 是 R 的一个实 Hensel 赋值环, 且它的剩余域是实闭域.

证明 由定理 8.5.1 的推论知, $A(Q)$ 是 R 的一个实 Hensel 赋值环. 设 v 是 $A(Q)$ 所对应的实赋值. 假若 v 的剩余域 R_v 不是实闭域, 则 R_v 有一个有限的实代数扩张 $R_v(\alpha)$, 使得 Q_v 可拓展为 $R_v(\alpha)$ 的一个普通序. 设 $\bar{f}(x)$ 是 α 在域 R_v 上的极小多项式, 则 $A(Q)[x]$ 中有一个首项系数为 1 的多项式 $f(x)$, 使得 $\bar{f}(x)$ 是 $f(x)$ 在自然同态: $A(Q)[x] \longrightarrow R_v[x]$ 下的象. 令 β 是 $f(x)$ 在 R 的代数闭包中的一个根, $K=R(\beta)$, 且 w 是 v 在域 K 上的一个拓展, 则显然 $\beta\in A_w$, 即 $\bar{\beta}:=\beta+M_w\in K_w$. 由命题 6.8.1 知, $[K:R]=[G_w:G_v][K_w:R_v]\geqslant[G_w:G_v][R_v(\bar{\beta}):R_v]$. 由于 $[K:R]=\deg(f(x))=\deg(\bar{f}(x))=[R_v(\bar{\beta}):R_v]$, 从而有 $[G_w:G_v]=1$, 且 $[K_w:R_v]=[R_v(\beta):R_v]$. 由此有 $K_w=R_v(\bar{\beta})\cong R_v(\alpha)$, 从而 Q_v 可拓展为 K_w 的一个普通序. 由定理 8.5.1 知, Q 可拓展为 K 的一个完全亚序, 矛盾于 "实闭包" 的定义. 因而, R_v 是一个实闭域. 证毕.

为进一步考虑 n 层序的实闭包, 我们需要下面的一个关于 Abel 群的引理.

引理 8.5.3 设 G 是一个运算为乘法的 Abel 群, $G^n:=\{g^n \mid g\in G\}$, 其中 $n\in\mathbb{N}$. 若 H 和 U 都是 G 的子群, 使得 $U\subseteq H$, H/U 是一个 n 阶循环群, 且 $G^n\cap H\subseteq U$, 则 G 有一个子群 V, 使得 (1)$G^n\subseteq V$, 且 $V\cap H=U$; (2)G/V 是一个 n 阶循环群.

证明 由 $G^n\cap H\subseteq U$ 可知, $G^nU\cap H=U$. 根据群的第二同构定理, $HG^n/G^nU\cong H/U$. 从而 HG^n/G^nU 是群 G/G^nU 的一个 n 阶循环子群. 记 $A=G/G^nU$, $B=HG^n/G^nU$. 借助于 Zorn 引理可知, A 有一个子群 C, 使得 C 关于条件: $B\cap C=\{1\}$ 是极大的. 此时, 可断言 $A=BC$. 事实上, 如若不然, 则 $A/C\neq BC/C$, 则有 $\bar{a}=aC\in A/C$, 使得 $\bar{a}\notin BC/C$. 令 m 为元素 $\bar{a}$ 的阶. 显然 $\bar{a}^n=\bar{1}$, 从而 $m\mid n$. 注意到 $\bar{a}^m=\bar{1}\in BC/C$. 从而可选取最小的自然数 k, 使得 $\bar{a}^k\in BC/C$. 易知, $k\mid m$. 于是, $\bar{a}^k$ 是子群 BC/C 中阶为 $\dfrac{m}{k}$ 的元素. 注意到 $BC/C\cong B/(B\cap C)\cong B$, 从而 BC/C 是一个 n 阶循环子群. 令 $\bar{b}:=bC$ 是 BC/C 的一个生成元且 $n=rm$, 其中 $b\in B$ 且 $r\in\mathbb{N}$, 则 $\bar{b}^{rk}$ 也是循环子群 BC/C 中阶为 $\dfrac{m}{k}$ 的元素. 从而必有 $\bar{a}^k=(\bar{b}^{rk})^s=(\bar{b}^{rs})^k$, 这里 $s\in\mathbb{N}$. 令 $d=b^{rs}a^{-1}$, 则显然 $d\notin C$. 容易证明: $C\cdot(d)\cap B=\{1\}$, 矛盾于 C 的极大性! 因而 $A=BC$. 由于 $A=G/G^nU$ 是群 G 的同态像, 从而 G 有一个子群 V, 使得 $G^nU\subseteq V$, 且

$C = V/G^nU$. 此时, $G/V \cong A/C = BC/C \cong B$, 即 G/V 是一个 n 阶循环群. 很清楚, $U \subseteq V \cap H$. 反过来, 若 $x \in V \cap H$, 则 $xG^nU \in C \cap B = \{1\}$, 即有 $x \in G^nU$. 由此有 $x \in G^nU \cap H$. 因而 $V \cap H = U$. 证毕.

引理 8.5.4 设 v 是域 F 的一个 Hensel 赋值, 且 v 的剩余域 F_v 是一个实闭域. 若 U 是乘法群 $\dot{F}$ 的一个子群, 使得 $-1 \notin U$, 且 $\dot{F}^{2m} \subseteq U$, 其中 $m \in \mathbb{N}$, 则 $U + U \subseteq U$.

证明 设 a, $b \in U$, 且不妨设 $v(a) \leqslant v(b)$, 则 $(a+b) = a(1+\alpha)$, 其中 $\alpha = ba^{-1} \in A_v \cap U$. 从而只须证明: $1+\alpha \in U$. 假若 $\bar{\alpha} = \alpha + M_v \notin F_v^2$, 则由 F_v 的实闭性知, $\bar{\alpha} \in -F_v^2 = -F_v^{2m}$. 考察多项式 $f(x) = x^{2m} + \alpha$, 则 $f(x)$ 在 $F_v[x]$ 中的像 $\bar{f}(x)$ 在 F_v 中有一个单根. 由 Hensel 引理知, $f(x)$ 在 A_v 中有一个根 c. 由此有 $-1 = \alpha(c^{-1})^{2m} \in U$, 矛盾. 从而 $\bar{\alpha} \in F_v^2$, 即有 $1 + \bar{\alpha} \in F_v^2 + F_v^2 = F_v^2 = F_v^{2m}$. 再根据 Hensel 引理可知, $1 + \alpha \in A_v^{2m} \subseteq U$. 证毕.

作为实闭域在高层序理论中的一个推广, 我们可以给出如下定义.

定义 8.5.3 设 Q 是域 R 的一个恰好层为 n 的序. 如果 Q 在 R 的每个真代数扩张上不能再拓展, 那么称 (R, Q) 是一个恰好层为 n 的实闭域.

显然, 若 Q 是域 R 的一个恰好层为 n 的序, 则 (R, Q) 是一个恰好层为 n 的实闭域, 当且仅当 (R, Q) 是它自身的实闭包. 现在, 我们着手考察恰好层为 n 的实闭域.

命题 8.5.5 设 (R, Q) 是一个恰好层为 n 的实闭域, G_v 是赋值环 $A(Q)$ 所对应的实赋值 v 的值群, 则下面的结论成立:

(1) $|\dot{R}/(\dot{R}^2 \cup -\dot{R}^2)| = 1$ 或 2, 且 $|\dot{R}/(\dot{R}^2 \cup -\dot{R}^2)| = 2$ 当且仅当 $2 \mid n$;

(2) 对于每个 $m \in \mathbb{N}$, 其中 m 的每个素因子都是 n 的因子, 则商群 $\dot{R}/(\dot{R}^m \cup -\dot{R}^m)$ 是一个 m 阶循环群;

(3) 对于与 n 互素的奇数 m, $R^m = R$;

(4) 对于每个素数 p, 当 $p \nmid n$ 时, $pG_v = G_v$; 当 $p \mid n$ 时, $|G_v/pG_v| = p$.

证明 (1),(2) 首先证明这样一个事实: 对于 $2n$ 的每个素因子 p, $Q \subseteq R^p \cup -R^p$. 事实上, 如若不然, 则有 $\alpha \in Q$, 使得 $\alpha \notin R^p \cup -R^p$. 此时可断定 $v(\alpha) \notin pG_v$. 否则, 有 $a \in R$, 使得 $v(\alpha) = pv(a)$, 即 $v(a^p\alpha^{-1}) = 0$. 由于 v 是剩余域为实闭域的 Hensel 赋值, 从而由 Hensel 引理知, $a^p\alpha^{-1} \in A_v^p \cup -A_v^p$, 即有 $\alpha \in R^p \cup -R^p$, 矛盾. 记 $\sqrt[p]{\alpha}$ 为多项式 $x^p - \alpha$ 在 R 的代数闭包中的一个根, 且 w 是 v 在域 $L = R(\sqrt[p]{\alpha})$ 上的惟一拓展. 注意到, $pw(\sqrt[p]{\alpha}) = w(\alpha) = v(\alpha) \in G_v$, 但 $w(\sqrt[p]{\alpha}) \notin G_v$ (否则 $v(\alpha) = pw(\sqrt[p]{\alpha}) \in pG_v$!). 因而, 由命题 6.8.1 知, $[L:R] = [F_w : F_v][G_w : G_v]$. 注意到 $[L:R] \leqslant p$, 且 $[G_w : F_v] \geqslant p$. 从而有 $[L:R] = [G_w : G_v] = p$, 且 $F_w = F_v$. 因而, w 是域 L 的一个实 Hensel 赋值, 且剩余域 F_w 是实闭域. 显然, $R^{2n} \cdot \langle \alpha^{\frac{2n}{p}} \rangle \subseteq L^{2n} \cap R$, 其中 $\langle \alpha^{\frac{2n}{p}} \rangle$ 是 $\dot{R}$ 中由 $\alpha^{\frac{2n}{p}}$ 生成的循环群. 反过来, 若 $x \in L^{2n} \cap R$, 且 $x \neq 0$, 则

$x = y^{2n}$, 其中 $y \in \dot{L}$. 注意到 $G_w = G_v + \langle w(\sqrt[p]{\alpha})\rangle$, 从而 $w(y) = v(b) + kw(\sqrt[p]{\alpha})$, 其中 $k \in \mathbb{Z}$, $b \in \dot{F}$. 此时有 $v(b^{2n}\alpha^{\frac{2kn}{p}}x^{-1}) = 0$. 显然, $b^{2n}\alpha^{\frac{2kn}{p}}x^{-1} \in L^{2n}$, 从而 $b^{2n}\alpha^{\frac{2kn}{p}}x^{-1} \in F_w^2 = F_v^2 = F_v^{2n}$. 由 Hensel 引理可知, $b^{2n}\alpha^{\frac{2kn}{p}}x^{-1} \in R^{2n}$, 即有 $x \in R^{2n} \cdot \langle \alpha^{\frac{2n}{p}}\rangle$. 因而, $L^{2n} \cap R = R^{2n} \cdot \langle \alpha^{\frac{2n}{p}}\rangle \subseteq Q$, 即 $\dot{L}^{2n} \cap \dot{R} \subseteq \dot{Q}$. 根据引理 8.5.3 知, 乘法群 $\dot{L}$ 有一个子群 $\dot{Q}_L$, 使得 $\dot{L}^{2n} \subseteq \dot{Q}_L$, $\dot{Q}_L \cap \dot{R} = \dot{Q}$, 且 $\dot{L}/\dot{Q}_L$ 是一个 $2n$ 阶循环群. 显然, $-1 \notin \dot{Q}_L$; 否则 $-1 \in \dot{Q}_L \cap R = \dot{Q}$! 再由引理 8.5.4 知, $Q_L := \dot{Q}_L \cup \{0\}$ 是 Q 在域 L 上的一个拓展, 与所设矛盾. 因此, 上面事实成立.

由上面事实可知, $\dot{R}/(\dot{R}^p \cup -\dot{R}^p)$ 是循环群 $\dot{R}/\dot{Q}$ 的同态象. 设 $a\dot{Q}$ 是循环群 $\dot{R}/\dot{Q}$ 的生成元, 其中 $a \in \dot{R}$, 则 $\dot{R}/(\dot{R}^p \cup -\dot{R}^p)$ 是一个由 $a(\dot{R}^p \cup -\dot{R}^p)$ 生成的循环群. 当 $p \neq 2$ 时, $R^p = -R^p$, 从而可知 $\dot{R}/\dot{R}^p$ 是一个阶为 p 的循环群. 当 $p = 2$ 时, $\dot{R}/(\dot{R}^2 \cup -\dot{R}^2)$ 的阶为 1 或 2. 显然, $\dot{R}/(\dot{R}^2 \cup -\dot{R}^2)$ 的阶为 2, 当且仅当 $2 \mid n$. 从而结论 (1) 成立.

再通过计算易知, 对于 n 的素因子 p 以及自然数 k. $\dot{R}/(\dot{R}^{p^k} \cup -\dot{R}^{p^k})$ 是一个由 $a(\dot{R}^{p^k} \cup -\dot{R}^{p^k})$ 生成的 p^k 阶循环群. 设 $m = p_1^{k_1} \cdots p_r^{k_r}$, 其中 $p_1, \cdots, p_r$ 是 n 的相异的素因子, $k_i \in \mathbb{N}$, $i = 1, \cdots, r$. 令 $H_i = \dot{R}/(\dot{R}^{p_i^{k_i}} \cup -\dot{R}^{p_i^{k_i}})$, 则 H_i 为 $p_i^{k_i}$ 阶循环群, $i = 1, \cdots, r$. 于是, 直积 $H_1 \times \cdots \times H_r$ 是一个阶为 m 的循环群. 作 $\dot{R}$ 到 $H_1 \times \cdots \times H_r$ 的如下映射:

$$\pi: \quad x \longmapsto \left(x(\dot{R}^{p_1^{k_1}} \cup -\dot{R}^{p_1^{k_1}}), \cdots, x(\dot{R}^{p_r^{k_r}} \cup -\dot{R}^{p_r^{k_r}})\right), \quad x \in \dot{R}.$$

显然, π 是一个群同态. 由于 $\pi(a)$ 是 $H_1 \times \cdots \times H_r$ 中一个阶为 m 的元素, 从而 π 是一个满同态. 通过计算易知, 同态核 $\ker(\pi)$ 恰为 $R^m \cup -R^m$. 由同态基本定理知, 结论 (2) 成立.

(3) 假若 $R \neq R^m$, 则对于 m 的某个素因子 p, $R \neq R^p$. 从而有 $\alpha \in R$, 使得 $\alpha \notin R^p$. 注意到 p 是奇素数. 从而由 Hensel 引理可知, $v(a) \notin pG_v$. 记 $\sqrt[p]{\alpha}$ 为多项式 $x^p - \alpha$ 在 R 的代数闭包中的一个根, 且 w 是 v 在域 $L = R(\sqrt[p]{\alpha})$ 上的惟一拓展. 通过上面类似的讨论可知, $G_w = G_v + < w(\sqrt[p]{\alpha}) >$. 设 $x \in L^{2n} \cap R$, 且 $x \neq 0$, 则 $x = y^{2n}$, 其中 $y \in \dot{L}$. 于是 $w(y) = v(b) + kw(\sqrt[p]{\alpha})$, 其中 $k \in \mathbb{Z}$, $b \in \dot{F}$. 于是有 $2nkw(\sqrt[p]{\alpha}) = v(xb^{-2n}) \in G_v$. 显然, $w(\sqrt[p]{\alpha}) \notin G_v$, 但 $pw(\sqrt[p]{\alpha}) = v(\alpha) \in G_v$. 注意到 p 与 $2n$ 互素, 从而易知 $p \mid k$, 即有 $\alpha^{\frac{2nk}{p}} \in R^{2n}$. 此时有 $v(b^{2n}\alpha^{\frac{2kn}{p}}x^{-1}) = 0$. 同样由 Hensel 引理可知, $b^{2n}\alpha^{\frac{2kn}{p}}x^{-1} \in R^{2n}$, 即有 $x \in R^{2n}$. 因而, $L^{2n} \cap R = R^{2n} \subseteq Q$. 由引理 8.5.3 知, Q 可以拓展为域 L 上一个恰好层为 n 的序, 矛盾. 因而, $R^m = R$.

(4) 设 p 是一个素数, 当 $p \nmid n$ 且 $p \neq 2$ 时, 由结论 (3) 知, $R^p = R$. 从而 $pG_v = G_v$. 当 $2 \nmid n$ 时, 由结论 (1) 知, $R = R^2 \cup -R^2$. 从而也有 $G_v = 2G_v$. 当 $p \mid n$ 时, 由结论 (2) 知, $\dot{R}/(\dot{R}^p \cup -\dot{R}^p)$ 是一个阶为 p 的循环群. 此时易见, $|G_v/pG_v| = 1$ 或 p. 如若 $G_v = pG_v$, 则由 Hensel 引理可知, $\dot{R} = \dot{R}^p \cup -\dot{R}^p$, 矛盾.

因此，$|G_v/pG_v| = p$. 至此，命题获证.

定理 8.5.6 设 (R, Q) 是一个恰好层为 n 的实闭域，则 R 的所有完全的高层亚序都为恰好层为 m 的序，其中 m 的每个素因子都整除 n，且

(1) 当 n 为奇数时，R 的恰好层为 m 的序正是子集 R^{2m};

(2) 当 n 为偶数时，R 的恰好层为 m 的序 P_{2m} 可通过这样的方式获得：若 m 为偶数，则 $P_{2m} = R^{2m} \cup -\alpha R^{2m}$，其中 $\alpha \in R^m$，但 $\alpha \notin R^{2m} \cup -R^{2m}$；若 m 为奇数，则 $P_{2m} = R^{2m} \cup \alpha R^{2m}$ 或 $P_{2m} = R^{2m} \cup -\alpha R^{2m}$，其中 $\alpha \in R^m$，但 $\alpha \notin R^{2m} \cup -R^{2m}$.

证明 设 P 是域 R 的任意一个恰好层为 m 的完全亚序，则由命题 8.5.5(3) 可知，m 的每个素因子都整除 n. 由命题 8.5.5(2) 知，$\dot{R}/(\dot{R}^m \cup -\dot{R}^m)$ 是一个 m 阶循环群.

当 n 为奇数时，$\dot{R}/\dot{R}^m$ 为 m 阶循环群. 由命题 8.5.5(1) 知，$\dot{R}/\dot{R}^2$ 是 2 阶循环群. 从而易知，$\dot{R}/\dot{R}^{2m}$ 为 $2m$ 阶循环群. 由于 $R^{2m} \subseteq P$，从而有 $P = R^{2m}$. 反过来，若自然数 m 的每个素因子都整除 n，则由上面讨论知，$\dot{R}/\dot{R}^{2m}$ 是一个 $2m$ 阶循环群. 由引理 8.5.4 知，$R^{2m} + R^{2m} \subseteq R^{2m}$. 因而，$R^{2m}$ 是 R 的一个恰好层为 m 的序.

当 n 为偶数时，由命题 8.5.5(2) 可知，$\dot{R}/(\dot{R}^m \cup -\dot{R}^m)$ 是一个 m 阶循环群，且 $\dot{R}/(\dot{R}^{2m} \cup -\dot{R}^{2m})$ 是一个 $2m$ 阶循环群. 显然 $R^m \not\subseteq R^{2m} \cup -R^{2m}$；否则，$\dot{R}/(\dot{R}^{2m} \cup -\dot{R}^{2m})$ 中每个元素的阶不超过 m. 对于 $\alpha \in R^m$，其中 $\alpha \notin R^{2m} \cup -R^{2m}$，$\alpha^2 \in R^{2m} \subseteq P$. 由 P 的完全性知，$\alpha \in P \cup -P$. 若 m 为偶数，则 $(R^{2m} \cup -R^{2m}) \cap R^m = R^{2m}$，即有 $R^m = R^{2m} \cup \alpha R^{2m}$. 假若 $\alpha \in P$，则 $R^m \subseteq P$，矛盾. 从而 $-\alpha \in P$. 此时易知，$P = R^{2m} \cup -\alpha R^{2m}$. 若 m 为奇数，则 $R^{2m} \cup -R^{2m} \subseteq R^m$. 此时，$R^m = R^{2m} \cup -R^{2m} \cup \alpha R^{2m} \cup -\alpha R^{2m}$. 由此可知，$P = R^{2m} \cup \alpha R^{2m}$ 或 $P = R^{2m} \cup -\alpha R^{2m}$. 反过来，设自然数 m 的每个素因子都整除 n，$\alpha \in R^m$，但 $\alpha \notin R^{2m} \cup -R^{2m}$. 由上面的讨论可知，当 m 为偶数时，$R^{2m} \cup -\alpha R^{2m}$ 为 R 的一个恰好层为 m 的序；而当 m 为奇数时，$R^{2m} \cup \alpha R^{2m}$ 和 $R^{2m} \cup -\alpha R^{2m}$ 都是 R 的恰好层为 m 的序. 证毕.

现在，我们可以给出高层实闭域的一个刻画，这个刻画可看做定理 3.4.9 的一个推广.

定理 8.5.7 设 Q 是域 R 的一个恰好层为 n 的序，G_v 是赋值环 $A(Q)$ 所对应的赋值 v 的值群，则 (R, Q) 是恰好层为 n 的实闭域，当且仅当如下三个条件都成立：

(1) v 是一个 Hensel 赋值;

(2) 对于素数 p，若 $p \nmid n$，则 $pG_v = G_v$；若 $p \mid n$，则 $|G_v/pG_v| = p$;

(3) v 的剩余域是一个实闭域.

证明 由定理 8.5.2 和命题 8.5.5 知，只须证明充分性. 为此，我们首先证明

$nG_v = v(\dot{Q})$.

设 $v(a) \in G_v$, 其中 $a \in \dot{R}$. 由于 $a^{2n} \in \dot{Q}$, 从而 $a^n \in \dot{Q} \cup -\dot{Q}$, 即有 $nv(a) \in v(\dot{Q})$. 因而, $nG_v \subseteq v(\dot{Q})$. 令 $n = p_1^{k_1} \cdots p_r^{k_r}$, 其中 $p_1, \cdots, p_r$ 为相异的素数, $k_i \in \mathbb{N}$, $i = 1, \cdots, r$. 由条件知, G_v/p_iG_v 为 p_i 阶循环群, $i = 1, \cdots, r$. 由此可知, $G_v/p_i^{k_i}G_v$ 为 $p_i^{k_i}$ 阶循环子群, $i = 1, \cdots, r$. 借助孙子定理可知, G_v/nG_v 与直和 $G_v/p_1^{k_1}G_v \oplus \cdots \oplus G_v/p_r^{k_r}G_v$ 同构, 从而 G_v/nG_v 是一个 n 阶循环群. 又由定理 8.3.6 知, $|G_v/v(\dot{Q})| = n$. 因而有 $v(\dot{Q}) = nG_v$.

假若 (R, Q) 不是一个恰好层为 n 的实闭域, 则 (R, Q) 有一个真有限扩张 (K, Q_K). 令 w 是赋值环 $A(Q_K)$ 所对应的赋值, 则 w 显然是 v 在 K 上的一个实拓展. 显然, w 也是一个 Hensel 赋值, 且它的剩余域 K_w 也是实闭域. 由命题 6.8.1 知, $[K : R] = [G_w : G_v][K_w : R_v] = [G_w : G_v]$, 即有 $G_w \neq G_v$. 显然 $v(\dot{Q}) \subseteq w(\dot{Q}_K) \cap G_v$. 若 $g \in w(\dot{Q}_K) \cap G_v$, 则 $g = w(\alpha) = v(a)$, 其中 $a \in \dot{R}$, 而 $\alpha \in \dot{Q}_K$. 由 Hensel 引理可知, $a\alpha^{-1} \in \dot{K}^{2n} \cup -\dot{K}^{2n} \subseteq \dot{Q}_K \cup -\dot{Q}_K$. 从而 $a \in (\dot{Q}_K \cup -\dot{Q}_K) \cap R = \dot{Q} \cup -\dot{Q}$, 即 $v(a) \in v(\dot{Q})$. 因而, $w(\dot{Q}_K) \cap G_v = v(\dot{Q})$. 根据定理 8.3.6 知, $[G_w : w(\dot{Q}_K)] = [G_v : v(\dot{Q})]$. 因而, $w(\dot{Q}_K) \nsubseteq G_v$; 否则 $w(\dot{Q}_K) = w(\dot{Q}_K) \cap G_v = v(\dot{Q})$! 从而有某个 $\alpha \in \dot{Q}_K$, 使得 $w(\alpha) \notin G_v$. 由于 K 是 R 的代数扩张, 从而有 $k \in \mathbb{N}$, 使得 $kw(\alpha) \in G_v$. 选取最小的自然数 k, 使得上面关系式成立. 必定 $k > 1$. 设 p 是 k 的一个素因子, 且令 $\beta = \alpha^{\frac{k}{p}}$, 则 $\beta \in \dot{Q}_K$, 使得 $w(\beta) \notin G_v$, 但 $pw(\beta) \in G_v$. 若 $p \nmid n$, 则 $pw(\beta) \in G_v = pG_v$. 此时有 $w(\beta) \in G_v$, 矛盾. 若 $p \mid n$, 则由上面讨论知, $pw(\beta) \in w(\dot{Q}_K) \cap G_v = v(\dot{Q}) = nG_v$. 此时, $w(\beta) \in \dfrac{n}{p}G_v \subseteq G_v$, 矛盾. 因而, (R, Q) 是一个恰好层为 n 的实闭域. 证毕.

§8.6 高层实全纯环

在 §3.5 中, 我们研究了实全纯环, 并获得实全纯环的一些重要特性. 对于一个 (普通的) 亚序域 (F, T) 以及 F 的一个子环 D, 我们把 F 的所有与 T 相容且包含 D 的实赋值环的交集称作 F 关于亚序 T 和子环 D 的实全纯环. 为了引进与高层亚序相关的实全纯环 (即高层实全纯环), 需要给出实赋值与高层亚序之间的相容性的定义.

定义 8.6.1 设 T 是域 F 的一个 n 层亚序, v 是 F 的一个赋值. 称 v 与 T 相容, 如果对于任意 $t_1, t_2 \in T$, $v(t_1 + t_2) = \min\{v(t_1), v(t_2)\}$. 此时, 亦称 v 的赋值环 A_v 与 T 相容.

显然, 上面的定义是定义 3.1.4 在高层亚序上的一个推广. 通过直接的常规验证可知, 若 T 是域 F 的一个 n 层亚序, 且 v 是 F 的一个与 T 相容的赋值, 则 v 的剩余域 F_v 的如下子集:

$$T_v = \{\bar{a} = a + M_v \mid a \in T \cap A_v\},$$

是 F_v 的一个 n 层亚序. 因而, 与亚序相容的赋值都是实的.

为了阐明定义 8.6.1 和定义 8.3.1 的一致性以及这两个定义之间的联系, 我们建立如下命题.

命题 8.6.1 设 T 是域 F 的一个 n 层亚序, v 是域 F 的一个赋值, 则

(1) 当 T 是完全亚序时, v 与 T 相容, 当且仅当 $1 + M_v \subseteq T$.

(2) v 与 T 相容, 当且仅当对于 F 的某个包含 T 的 n 层序 P, v 与 P 相容.

证明 (1) 设 $1 + M_v \subseteq T$. 假若 v 与 T 不相容, 则有 $t_1, t_2 \in T$, 使得 $v(t_1 + t_2) > \min\{v(t_1), v(t_2)\}$. 此时必有 $v(t_1) = v(t_2)$, 且 t_1 和 t_2 都不为零. 从而有 $(t_1 + t_2)t_1^{-1} \in M_v$. 由所设知, $1 - (t_1 + t_2)t_1^{-1} \in T$, 即 $-t_2t_1^{-1} \in T$. 由此有 $-1 = (-t_2t_1^{-1})t_1t_2^{-1} \in T$, 矛盾. 因而, v 与 T 相容.

反过来, 设 v 与 T 相容. 根据定理 8.3.3 知, $A(T) = \{a \in F \mid 有 m \in \mathbb{N}, 使得 m \pm a \in T\}$ 是 F 的一个实赋值环, 使得 $1 + I(T) \subseteq T$, 这里 $I(T)$ 是 $A(T)$ 的极大理想. 对于 $a \in A(T)$, 有 $m \in \mathbb{N}$, 使得 $m \pm a \in T$. 由 v 与 T 的相容性知, $v(m+a) \geqslant \min\{v(m+a), v(m-a)\} = v\big((m+a)+(m-a)\big) = v(2m) = v(1) = 0$. 此时必有, $v(a) \geqslant 0$, 即 $a \in A_v$. 这表明 $A(T) \subseteq A_v$. 因而, $1 + M_v \subseteq 1 + I(T) \subseteq T$.

(2) 设 P 是 F 的一个 n 层序, 使得 $T \subseteq P$, 且 v 与 P 相容. 由定义 8.6.1 知, 显然 v 与 T 相容.

现设 v 与 T 相容. 令 $T_1 = \left\{\sum_{i=1}^{m} t_i(1+\eta_i) \mid m \in \mathbb{N}, t_i \in T, \eta_i \in M_v\right\}$. 显然 $T \subseteq T_1$, $T_1 + T_1 \subseteq T_1$, 且 $T_1 \cdot T_1 \subseteq T_1$. 如若 $-1 \in T_1$, 则 $-1 = \sum_{i=1}^{m} t_i(1+\eta_i)$, 其中 $t_i \in T$, $\eta_i \in M_v$, $i = 1, \cdots, m$. 令 $a = 1 + \sum_{i=1}^{m} t_i = -\sum_{i=1}^{m} t_i\eta_i$, 则可导致如下矛盾:

$$\begin{aligned} v(a) &= v\left(\sum_{i=1}^{m} t_i\eta_i\right) \geqslant \min\{v(t_1\eta_1), \cdots, v(t_m\eta_m)\} \\ &> \min\{v(1), v(t_1), \cdots, v(t_m)\} = v(a). \end{aligned}$$

从而 $-1 \notin T_1$. 这表明 T_1 也是 F 的一个 n 层亚序. 由定理 8.3.7 知, F 有一个 n 层序 P, 使得 $T_1 \subseteq P$. 注意到 $1 + M_v \subseteq T_1 \subseteq P$, 从而 v 与 P 相容. 此时, 显然 $T \subseteq P$. 证毕.

类似于定义 3.5.1, 我们给出高层实全纯环 的如下定义.

定义 8.6.2 设 T 是域 F 的一个 n 层亚序, D 是 F 的一个子环. F 的所有与 T 相容且包含 D 的赋值环之交集称作 F 关于亚序 T 和子环 D 的实全纯环, 且记作 $H_F(T, D)$. 特别地, 当 $D = \mathbb{Q}$ 时, 相应的实全纯环迳称作 F 关于亚序 T 的

实全纯环，且简记作 $H_F(T)$.

设 D 是域 F 的一个子环，且 P 是 F 的一个 n 层序，则可构造 F 的如下子集：

$$C(D,P)=\{x\in F \mid 有 d\in D\cap\sum F^{2n}，使得 d\pm x\in P\}.$$

对于上面的子集 $C(D,P)$, 我们有如下结论.

命题 8.6.2 设 P 是域 F 的一个 n 层序，D 是 F 的一个子环，则 $C(D,P)$ 是 F 的一个与 P 相容且包含子环 D 的赋值环，且它包含在 F 的每个与 P 相容且包含 D 的赋值环中.

证明 由恒等式

$$(2n)!x=\sum_{k=0}^{2n-1}(-1)^{k+1}\binom{2n-1}{k}[(x+k)^{2n}-k^{2n}]$$

可知，对于每个 $y\in D$, $(2n)!y=t_1-t_2$, 其中 $t_1,t_2\in D\cap\Sigma F^{2n}$. 令 $d=t_1+t_2\in D\cap P$, 则 $(2n)!(d\pm y)\in P$, 即有 $y\in C(D,P)$. 因而，$D\subseteq C(D,P)$.

设 x, $y\in C(D,P)$, 则有 d_1, $d_2\in D\cap\Sigma F^{2n}$, 使得 $d_1\pm x$, $d_2\pm y\in P$. 从而 $(d_1+d_2)\pm(x-y)=(d_1\pm x)+(d_2\mp y)\in P$, 即有 $x-y\in C(D,P)$. 此外，$d_1d_2\pm xy=\dfrac{1}{2}(d_1+x)(d_2\pm y)+\dfrac{1}{2}(d_1-x)(d_2\mp y)\in P$, 即有 $xy\in C(D,P)$. 因而，$C(D,P)$ 是域 F 的一个子环.

注意到 $\mathbb{N}\subseteq D\cap\Sigma F^{2n}$, 从而 $A(P)\subseteq C(D,P)$. 由于 $A(P)$ 是 F 的一个赋值环，从而 $C(D,P)$ 也是 F 的一个赋值环，使得 $M_2\subseteq M_1$, 这里 M_1 和 M_2 分别为 $A(P)$ 和 $C(D,P)$ 的极大理想. 由 $A(P)$ 与 P 的相容性知，$1+M_2\subseteq 1+M_1\subseteq P$. 于是，赋值环 $C(D,P)$ 与 P 相容.

再设 B 是 F 的任意一个与 P 相容且包含 D 的赋值环，且 v 为 B 所对应的赋值. 对于 $x\in C(D,P)$, 有 $d\in D\cap\Sigma F^{2n}$, 使得 $d\pm x\in P$. 从而 $v(d+x)\geqslant \min\{v(d+x),v(d-x)\}=v\big((d+x)+(d-x)\big)=v(2d)\geqslant 0$. 此时必有 $v(x)\geqslant 0$, 即 $x\in B$. 因而，$C(D,P)\subseteq B$. 命题获证.

根据上面两个命题，容易建立下面的定理：

定理 8.6.3 设 T 是域 F 的一个 n 层亚序，D 是 F 的一个子环，则

$$H_F(T,D)=\bigcap C(D,P),$$

这里 P 取遍 F 的所有包含 T 的 n 层序.

证明 由命题 8.6.2 知，对于 F 的每个包含 T 的 n 层序 P, $C(D,P)$ 是 F 的一个与 P 相容且包含 D 的赋值环. 再由命题 8.6.1 知，$C(D,P)$ 与 T 相容. 由 $H_F(T,D)$ 的定义知，$H_F(T,D)\subseteq\bigcap C(D,P)$, 其中 P 取遍 F 的所有包含 T 的 n

层序.

另一方面，若 B 是 F 的任意一个与 T 相容且包含 D 的赋值环，则由命题 8.6.1 知， B 与 F 的某个包含 T 的 n 层序 P_1 相容. 根据命题 8.6.1 知， $B \supseteq C(D,P_1) \supseteq \bigcap C(D,P)$, 其中 P 取遍 F 的所有包含 T 的 n 层序. 由 B 的任意性知， $H_F(T,D) \supseteq \bigcap C(D,P)$, 其中 P 取遍 F 的所有包含 T 的 n 层序. 证毕.

为了进一步刻画高层实全纯环 $H_F(T,D)$ 中的元素，我们需要把域 F 的所有包含 T 的 n 层序作为一个拓扑空间来加以研究. 设 T 是域 F 的一个 n 层亚序，且用 $\mathcal{X}_F(T)$ 表示 F 的所有包含 T 的 n 层序组成的集合. 再令 ξ 是复数域中一个 $2n$ 次本原单位根，则 $\Gamma = \{\xi, \cdots, \xi^{2n}\}$ 是一个由 ξ 生成的 $2n$ 阶 (乘法) 循环群. 对于每个 $P \in \mathcal{X}_F(T)$, 由命题 8.2.5 知， $\dot{F}/\dot{P}$ 是一个阶为 $2m$ 的循环群，其中 m 为 n 的一个因子. 从而有一个群同态 μ_P: $\dot{F}/\dot{P} \longrightarrow \Gamma$. 将自然同态： $\dot{F} \longrightarrow \dot{F}/\dot{P}$ 与 μ_P 合成，则得群同态 λ_P: $\dot{F} \longrightarrow \Gamma$, 使得对于 $a \in \dot{F}$, $\lambda_P(a) = \xi^{2n} = 1$ 当且仅当 $a \in \dot{P}$.

赋予 Γ 以离散拓扑, 则由熟知的 Tychonoff 定理, 乘积空间 $\Gamma^{\dot{F}}$ 是一个 Hausdorff 的紧空间. 显然，对于每个 $P \in \mathcal{X}_F(T)$, $\lambda_P \in \Gamma^{\dot{F}}$. 考察 $\mathcal{X}_F(T)$ 到 $\Gamma^{\dot{F}}$ 的如下映射：

$$\lambda: \qquad P \longmapsto \lambda_P, \quad P \in \mathcal{X}_F(T).$$

显然， λ 是一个单射. 通过类似于定理 1.5.3 的证明可知，映射 λ 的象 $\lambda(\mathcal{X}_F(T))$ 是拓扑空间 $\Gamma^{\dot{F}}$ 的一个闭子集. 从而 $\lambda(\mathcal{X}_F(T))$ 是一个紧子空间.

将 $\mathcal{X}_F(T)$ 与 $\lambda(\mathcal{X}_F(T))$ 等同，从而使得 $\mathcal{X}_F(T)$ 是一个 Hausdorff 的紧空间. 根据乘积拓扑的定义可知，所得的拓扑空间 $\mathcal{X}_F(T)$ 的一个子基由所有如下子集组成：

$$H(a;k) = \{P \in \mathcal{X}_F(T) \mid \lambda_P(a) = \xi^k\},$$

其中 $a \in \dot{F}$, $k = 1, \cdots, 2n$. 由这样一个子基所确定的拓扑称作 $\mathcal{X}_F(T)$ 的 Tychonoff 拓扑 .

鉴于拓扑空间 $\mathcal{X}_F(T)$ 的紧致性，我们可以对高层实全纯环的元素进行如下刻画.

定理 8.6.4 所设同定理 8.6.3, 且 $x \in F$, 则 $x \in H_F(T,D)$, 当且仅当有某个 $d \in D$, 使得 $d \pm x \in T$.

证明 设 $d \pm x \in T$, 其中 $d \in D$, 则对于 F 的每个包含 T 的 n 层序 P, 显然有 $x \in C(D,P)$. 由定理 8.6.3 知， $x \in H_F(T,D)$.

现设 $x \in H_F(T,D)$, 则由定理 8.6.3 知，对于 F 的每个包含 T 的 n 层序 P, $x \in C(D,P)$. 于是, 对于每个 $P \in \mathcal{X}_F(T)$, 有 $d_P \in D \cap \Sigma F^{2n}$, 使得 $d_P \pm x \in P$. 对于每个 $P \in \mathcal{X}_F(T)$, 令 $H_P = H(d_P+x;2n) \cap H(d_P-x;2n) = \{Q \in \mathcal{X}_F(T) \mid d_P \pm x \in Q\}$,

则对于 $\mathcal{X}_F(T)$ 的 Tychonoff 拓扑，H_P 是一个开子集. 这样，我们得到 $\mathcal{X}_F(T)$ 的一个开复盖 $\{H_P \mid P\in\mathcal{X}_F(T)\}$. 由 $\mathcal{X}_F(T)$ 的紧性知，$\mathcal{X}_F(T)$ 有一个有限的子复盖 $\{H_{P_i}\mid P_i\in\mathcal{X}_F(T), i=1,\cdots,r\}$. 令 $d=\sum_{i=1}^{r} d_{P_i}$, 则显然 $d\in D\cap\Sigma F^{2n}$. 此时，对于每个 $P\in\mathcal{X}_F(T)$, 有某个 $k\in\{1,\cdots,r\}$, 使得 $P\in H_{P_k}$, 即 $d_{P_k}\pm x\in P$. 从而, $d\pm x=(d_{P_k}\pm x)+(d-d_{P_k})\in P+T\subseteq P$. 根据定理 8.3.7, 我们有 $d\pm x\in T$. 证毕.

在定理 8.6.4 的基础上，可进一步建立下面的定理，这一定理给出了高层实全纯环 $H_F(T,D)$ 中元素的形式.

定理 8.6.5 所设同定理 8.6.4, 则对于 $x\in F$, 下列叙述等价:

(1) $x\in H_F(T,D)$;

(2) 对于某个 $t\in T$, $x^{2n}+t\in D$;

(3) $x\in D\left[\frac{1}{1+t}\mid t\in T\right]$, 这里 $D\left[\frac{1}{1+t}\mid t\in T\right]$ 表示将子集 $\left\{\frac{1}{1+t}\mid t\in T\right\}$ 添加到子环 D 上所得的扩环.

证明 (1) $\Longleftrightarrow$ (2): 设 $x\in H_F(T,D)$, 则显然 $x^{2n}\in H_F(T,D)$. 由定理 8.6.4 知，有 $d\in D$, 使得 $d-x^{2n}\in T$. 令 $t=d-x^{2n}$, 则 $t\in T$, 使得 $x^{2n}+t\in D$.

再设 $x^{2n}+t\in D$, 其中 $t\in T$. 对于 F 的任意一个与 T 相容且包含 D 的赋值环 B, 用 v_B 表示 B 所对应的赋值. 此时，$v_B(x^{2n})\geqslant\min\{v_B(x^{2n}),v_B(t)\}=v_B(x^{2n}+t)\geqslant 0$. 从而 $x^{2n}\in B$, 即 $x\in B$. 由 $H_F(T,D)$ 的定义知，$x\in H_F(T,D)$.

(1) $\Longleftrightarrow$ (3): 设 $x\in H_F(T,D)$, 则由定理 8.6.4 知，有 $d\in D$, 使得 $d\pm x\in T$. 令 $t_1=d+x$, 且 $t_2=d-x$, 则 $t_1, t_2\in T$, 且 $(1+t_1)(d+1-x)=(1+t_2)(d+1+x)$. 由此有，$x=(d+1)\left(\frac{1+t_1}{2+t_1+t_2}-\frac{1+t_2}{2+t_1+t_2}\right)$. 令 $t=\frac{1+t_1}{1+t_2}$, 则 $t, t^{-1}\in T$. 从而 $x=(d+1)\left(\frac{1}{1+t^{-1}}-\frac{1}{1+t}\right)\in D\left[\frac{1}{1+t}\mid t\in T\right]$.

再设 $x\in D\left[\frac{1}{1+t}\mid t\in T\right]$. 对于 F 的任意一个与 T 相容且包含 D 的赋值环 B, 仍用 v_B 表示 B 所对应的赋值. 此时，对于每个 $t\in T$, $v_B(1+t)=\min\{v_B(1),v_B(t)\}\leqslant v(1)=0$, 即 $v_B\left(\frac{1}{1+t}\right)=-v_B(1+t)\geqslant 0$. 从而 $\frac{1}{1+t}\in B$. 于是 $D\left[\frac{1}{1+t}\mid t\in T\right]\subseteq B$, 即有 $x\in B$. 因此，$x\in H_F(T,D)$. 证毕.

推论 设 D 是实域 F 的一个子环，则对于每个自然数 n, $H_F(\Sigma F^2,D)=H_F(\Sigma F^{2n},D)$.

证明 注意到，F 的每个与 ΣF^{2n} 相容的赋值都是实赋值，从而它与 ΣF^2 相容. 于是有，$H_F(\Sigma F^2,D)\subseteq H_F(\Sigma F^{2n},D)$. 又由于 $\Sigma F^{2n}\subseteq\Sigma F^2$, 从而由定理 8.6.5 知，$H_F(\Sigma F^{2n},D)=D\left[\frac{1}{1+t}\mid t\in\Sigma F^{2n}\right]\subseteq D\left[\frac{1}{1+t}\mid t\in\Sigma F^2\right]=H_F(\Sigma F^2,D)$.

证毕.

引理 8.6.6 所设同定理 8.6.5, 则 F 的每个包含 $H_F(T,D)$ 的赋值环都与 T 相容.

证明 设 B 是 F 的任意一个包含 $H_F(T,D)$ 的赋值环, 且 v 是 B 所对应的赋值. 对于任意非零的 $t_1, t_2 \in T$, 其中 $v(t_1) \leqslant v(t_2)$, $1+t_1^{-1}t_2 \in B$. 此外, 由定理 8.6.5 知, $\dfrac{1}{1+t_1^{-1}t_2} \in H_F(T,D) \subseteq B$. 从而 $v(1+t_1^{-1}t_2)=0$. 此时有, $v(t_1+t_2)=v(t_1)+v(1+t_1^{-1}t_2)=v(t_1)=\min\{v(t_1),v(t_2)\}$. 因此, B 与 T 相容. 证毕.

为了研究高层实全纯环 $H_F(T,D)$ 的局部化, 我们需要一个引理, 这一引理可看做 Dress 引理 (引理 3.5.5) 的一个推广.

引理 8.6.7 设 F 是一个特征为零的域, H 是 F 的一个包含 $\mathbb{Q}$ 的子环, 且 $r \in \mathbb{N}$. 若对于每个 $y \in F$, $(1+y^r)^{-1} \in H$, 只要 $1+y^r \neq 0$, 则对于 H 的每个素理想 $\wp$, H 关于 $\wp$ 的局部化为域 F 的一个赋值环.

证明 不妨直接设 H 是 F 的一个局部子环, 从而只须证明: H 是 F 的一个赋值环. 令 M 为 H 的极大理想. 首先, 我们证明如下断言.

断言 1 对于 $a \in \dot{F}$, $a^r \in H$ 或 $a^{-r} \in H$.

事实上, 如若 $a^r \notin H$, 则 $1+a^r \notin H$. 由于 $(1+a^r)^{-1} \in H$, 从而 $(1+a^r)^{-1} \in M$. 于是 $1-(1+a^r)^{-1} \in H \setminus M$, 即 $a^r(1+a^r)^{-1} \in H \setminus M$. 由此有 $1+a^{-r}=[a^r(1+a^r)^{-1}]^{-1} \in H$, 即有 $a^{-r} \in H$.

令 C 为 H 在 F 中的整闭包, 则可证明如下断言.

断言 2 C 是 F 的一个赋值环, 使得对于每个 $c \in C$, $c^r \in H$.

事实上, 对于每个 $a \in \dot{F}$, 由断言 1 知, $a^r \in H$ 或 $a^{-r} \in H$. 从而 $a \in C$ 或 $a^{-1} \in C$. 这表明 C 是 F 的一个赋值环. 假若对于某个 $c \in C$, $c^r \notin H$, 则 $c^{-r} \in H \subseteq C$. 于是, c^r 是 C 中可逆元. 令 M_C 为 C 的极大理想, 则由 C 在 H 上的整性知, $M_C \cap H = M$. 显然, $c^{-r} \notin M_C$, 自然有 $c^{-r} \notin M$. 由 H 的局部性知, $c^r=(c^{-r})^{-1} \in H$, 矛盾. 因而, 断言 2 成立.

只剩下证明: $C \subseteq H$. 由断言 2 可知, 对于每个 $c \in C$,

$$(2r)!c=\sum_{k=0}^{2r-1}(-1)^{k+1}\binom{2r-1}{k}[(c+k)^{2r}-k^{2r}] \in H.$$

从而即有 $c \in H$. 至此, 引理获证. 证毕.

借助于引理 8.6.6 和引理 8.6.7, 可将定理 3.5.6 推广如下.

定理 8.6.8 设 T 是域 F 的一个 n 层亚序, D 是 F 的一个子环, 则实全纯环 $H:=H_F(T,D)$ 的所有素理想与 F 的所有与 T 相容且包含 D 的赋值环之间存

在这样的一一对应: $\wp \longmapsto H_\wp$, 其中 $\wp$ 是 H 的素理想, 而 $H_\wp$ 为 H 关于 $\wp$ 的局部化.

证明 照搬定理 3.5.6 的证明即可.

第九章　一些构造性结论

在前面的各章中，除少数结果外 (例如 Sylvester 定理，Sturm 定理，定理 2.5.4 和 Tarski-Seidenberg 原理等)，绝大部分结论都是非构造性的．这些非构造性的结论都是在给定的假设条件下，通过逻辑推理而演绎出的定理、命题与推论．然而，数学结论还包括一类在理论和实践上都十分有意义的结论 —— 构造性结论．这些构造性的结论是通过一些切实可行的有效算法，来判定所研究的对象是否具有某种特定性质或者计算出所求对象的具体形式．

在本章中，我们将建立一些与实域理论有关的构造性结果，比如代数方程组有实解的判定，半定多项式的判定，多项式理想实根的计算，正定齐次多项式的平方和有效表示以及柱形代数分解等．理论上，所涉及的许多问题都可借助 Tarski-Seidenberg 原理来解决．然而，Tarski-Seidenberg 原理将导出太多的由等式和不等式所构成的关系式组，以致问题的处理难以实施．借助计算机代数系统，本章所提供的方法可处理有关的实例．

本章的内容涉及到其他有关理论和计算方法．限于篇幅，这些理论和方法不能详述．因而，在必要论及某个理论和方法时，将指明其出处以供查考．

§9.1　实多项式方程有解的非标准判定

判定实多项式方程是否有实解，是实代数几何在计算方面的一个基本重要课题，这一课题与有序几何中定理机器证明密切相关．本节突破给定多项式所在的原来系数域的局限，将问题的讨论从原系数域扩大到一个可计算的包含无限小元素的非阿基米德序域．正因为这一缘故，称本节中的方法是非标准的．

依照文献 [22] 中定义 4.18，一个序域 $(F,\leqslant)$ 称作可计算的，如果 F 是一个可计算域，且 $\leqslant$ 是 F 的一个可判定序．设 $t:=t_1,\cdots,t_n$ 是域 F 上 n 个未定元，且令 $F_{\langle n\rangle}=F(t_1,\cdots,t_n)$．由定理 2.6.4 可知，序 $\leqslant$ 可以惟一地拓展成域 $F_{\langle n\rangle}$ 的一个序，仍记作 $\leqslant$，使得 t_1 在 F 上是正的无限小，且 t_i 在 $F_{\langle i-1\rangle}$ 上是正的无限小，$i=2,\cdots,n$．显然，序域 $(F_{\langle n\rangle},\leqslant)$ 也是可计算的．事实上，对于 $F_{\langle n\rangle}$ 中非零元素 $\dfrac{f}{g}$，其中 f,g 为 $F[t_1,\cdots,t_n]$ 中非零多项式，$\dfrac{f}{g}<0$ 当且仅当多项式 fg 关于字典序 $t_1\prec t_2\prec\cdots\prec t_n$ 的尾项系数为负．用 R 和 $R_{\langle n\rangle}$ 分别表示序域 $(F,\leqslant)$ 和 $(F_{\langle n\rangle},\leqslant)$ 的实闭包．当然，认定 $R\subseteq R_{\langle n\rangle}$．此外，用 $R_{\langle i\rangle}$ 表示 $F_{\langle i\rangle}$ 在 $R_{\langle n\rangle}$ 中的代数闭包，$i=1,\cdots,n-1$．由命题 2.1.5 知，$R_{\langle i\rangle}$ 实际上也是 $F_{\langle i\rangle}$ 关于序 $\leqslant$ 的实闭包．显然 $R\subset R_{\langle 1\rangle}\subset\cdots\subset R_{\langle n\rangle}$．

作实闭域 $R_{\langle n\rangle}$ 的如下两个子集:

$$A_{\langle n\rangle}=\{z\in R_{\langle n\rangle}\mid 对于R中某个正元素d,\ -d\leqslant z\leqslant d\};$$
$$M_{\langle n\rangle}=\{z\in R_{\langle n\rangle}\mid 对于R中任意正元素d,\ -d\leqslant z\leqslant d\}.$$

由序 $\leqslant$ 的结构可知 $R\subseteq A_{\langle n\rangle}$, 且 $t_i\in M_{\langle n\rangle}$, $i=1,\cdots,n$. 根据实赋值的熟知结论, $A_{\langle n\rangle}$ 是域 $R_{\langle n\rangle}$ 的一个实赋值环, $M_{\langle n\rangle}$ 是 $A_{\langle n\rangle}$ 的赋值理想. 此外, $A_{\langle n\rangle}$ 和序 $\leqslant$ 是相容的. 由命题 3.1.3 知, $A_{\langle n\rangle}$ 和 $M_{\langle n\rangle}$ 关于序 $\leqslant$ 都是 $R_{\langle n\rangle}$ 的凸子集. 注意到剩余域 $A_{\langle n\rangle}/M_{\langle n\rangle}$ 同构于 R, 从而存在一个从 $A_{\langle n\rangle}$ 到 R 的同态 π, 使得对于每个 $f\in R[t_1,\cdots,t_n]$, $\pi(f)=f(0,\cdots,0)$.

在本节中, 将使用上述术语和记号, 不再另加说明.

现设 $f\in F[\overline{X}]:=F[x_1,\cdots,x_n]$ 是一个正次数 n 元多项式. 对于 $i=1,\cdots,n$, 作 R 的如下子集: $\mathcal{V}_R(f;x_i)=\{a_i\in R\mid 有a_1,\cdots,a_{i-1},a_{i+1},\cdots,a_n\in R,使得f(a_1,\cdots,a_{i-1},a_i,a_{i+1},\cdots,a_n)=0\}$. 由文献 [25] 中命题 2.1.7 知, 当方程 $f=0$ 在 R 中有解时, 所有的 $\mathcal{V}_R(f;x_i)$ 都是 R 的非空半代数子集, 且都是由 R 中有限个不相交的 (开或闭或半开半闭) 区间以及点构成的并集. 对于 $a\in R$, 记 $[a,a]=\{a\}$, 即单点集可看作左, 右端点相同的闭区间. 如若 $\mathcal{V}_R(f;x_i)$ 有某两个区间, 其中一个的右端点和另一个的左端点相同, 且一开一闭, 则可将两者合并为一个大区间. 因此, 总假定 $\mathcal{V}_R(f;x_i)$ 中任何两个区间都不具有如此情形, $i=1,\cdots,n$. 一个区间的端点 a 称作有限端点, 若 $a\neq-\infty$ 且 $a\neq+\infty$. 显然, 当 $\mathcal{V}_R(f;x_i)\neq R$ 时, $\mathcal{V}_R(f;x_i)$ 必有有限端点. 对于有限端点, 有如下断言.

引理 9.1.1 设 a_1 是 $\mathcal{V}_R(f;x_1)$ 的一个有限闭端点, 且 $a_2,\cdots,a_n\in R$, 使得 $f(a_1,a_2,\cdots,a_n)=0$, 则方程组

$$\begin{cases} f &=0,\\ \dfrac{\partial f}{\partial x_i} &=0, \quad i=2,\cdots,n \end{cases}$$

在 R 中有解 $(a_1,a_2,\cdots,a_n)$.

证明 由于端点 a_1 不是 $\mathcal{V}_R(f;x_1)$ 的内点, 从而对于 a_1 的任意开邻域 S, 均有 $S\not\subseteq\mathcal{V}_R(f;x_1)$. 假若对于某个 $j\in\{2,\cdots,n\}$, $\dfrac{\partial f}{\partial x_j}(a_1,\cdots,a_n)\neq 0$. 不失一般性, 不妨设 $j=n$. 根据适合实闭域的隐函数定理 (参见定理 7.4.5), 存在 $(a_1,\cdots,a_{n-1})$ 在拓扑空间 R^{n-1} 中的一个开邻域 Δ, a_n 在 R 中的一个开邻域 T 以及一个从 Δ 到 T 的函数 (映射)ψ, 使得 $\psi(a_1,\cdots,a_{n-1})=a_n$, 且对于每个 $(x_1,\cdots,x_{n-1},x_n)\in\Delta\times T$, $f(x_1,\cdots,x_{n-1},x_n)=0$ 当且仅当 $\psi(x_1,\cdots,x_{n-1})=x_n$. 由空间 R^{n-1} 的拓扑结构, 存在点 a_i 在 R 中的一个开邻域 S_i, $i=1,\cdots,n-1$, 使得 $S_1\times\cdots\times S_{n-1}\subseteq\Delta$. 这样, 显然有 $S_1\subseteq\mathcal{V}_R(f;x_1)$, 矛盾. 因此, 对于每个 $i=2,\cdots,n$, $\dfrac{\partial f}{\partial x_i}(a_1,\cdots,a_n)=0$. 证毕.

引理 9.1.2 设 $\mathcal{V}_R(f;x_1)$ 有一个有限开端点, 则对于某个 $j\in\{2,\cdots,n\}$, 方程

$$f(x_1,\cdots,x_{j-1},t^{-1},x_{j+1},\cdots,x_n)=0$$

或

$$f(x_1,\cdots,x_{j-1},-t^{-1},x_{j+1},\cdots,x_n)=0$$

在 $R_{\langle 1\rangle}$ 中有解.

证明 不失一般性, 设 a_1 是 $\mathcal{V}_R(f;x_1)$ 的一个左侧有限开端点, 则 $a_1\notin\mathcal{V}_R(f;x_1)$, 同时必有一个开区间 $]a_1,c[$ 包含在 $\mathcal{V}_R(f;x_1)$ 中, 其中 $c\in R$, 使得 $a_1<c$. 此时, 可以断言: 对于某个 $j\in\{2,\cdots,n\}$, $\mathcal{V}_R(f;x_j)$ 不是一个有界集. 事实上, 如若不然, 则 R 中存在一个正元素 d, 使得对于任意 $y\in\mathcal{V}_R(f;x_i)$, $i=2,\cdots,n$, 总有 $-d<y<d$. 于是, 如下语句在 R 中成立:

$$\forall x_1(a_1<x_1<c)\longrightarrow\exists(x_2,\cdots,x_n)\big(f(x_1,x_2,\cdots,x_n)=0\vee -d<x_2<d\vee\cdots\vee -d<x_n<d\big).$$

注意到 $R\subseteq R_{\langle 1\rangle}$. 由转移定理知, 上面语句在 $R_{\langle 1\rangle}$ 中也成立. 令 $\alpha_1=a_1+t$, 则 $\alpha_1\in R_{\langle 1\rangle}$, 且 $a_1\langle\alpha_1\rangle c$. 于是存在 $\alpha_2,\cdots,\alpha_n\in R_{\langle 1\rangle}$, 使得 $f(\alpha_1,\cdots,\alpha_n)=0$, 且 $-d<\alpha_i<d$, $i=2,\cdots,n$. 由赋值环 $A_{\langle 1\rangle}$ 的结构, 有 $\alpha_i\in A_{\langle 1\rangle}$, $i=1,\cdots,n$. 于是 $f(\pi(\alpha_1),\cdots,\pi(\alpha_n))=\pi(f(\alpha_1,\cdots,\alpha_n))=0$, 即 $f(a_1,\cdots,\pi(\alpha_n))=0$, 这里 $\pi(\alpha_i)\in R$, $i=2,\cdots,n$. 从而有 $a_1\in\mathcal{V}_R(f;x_1)$, 矛盾. 由于 $\mathcal{V}_R(f;x_j)$ 不是有界集, 从而它必有一个区间以 $+\infty$ 或 $-\infty$ 为端点. 如果 $+\infty$ 是 $\mathcal{V}_R(f;x_j)$ 的某个区间的端点, 则必存在 $c\in R$, 使得 $]c,+\infty[\subseteq\mathcal{V}_R(f;x_j)$. 从而, 有如下语句在 R 中成立:

$$\forall x_j(c<x_j)\longrightarrow\exists(x_1,\cdots,x_{j-1},x_{j+1},\cdots,x_n)\big(f(x_1,x_2,\cdots,x_n)=0\big).$$

由转移定理, 上面语句在 $R_{\langle 1\rangle}$ 中也成立. 注意到, $t^{-1}\in R_{\langle 1\rangle}$ 且 $c<t^{-1}$. 从而方程 $f(x_1,\cdots,x_{j-1},t^{-1},x_{j+1},\cdots,x_n)=0$ 在 $R_{\langle 1\rangle}$ 中有解.

当 $-\infty$ 为 $\mathcal{V}_R(f;x_j)$ 的某个区间的端点时, 我们可以类似地证明方程

$$f(x_1,\cdots,x_{j-1},-t^{-1},x_{j+1},\cdots,x_n)=0$$

在 $R_{\langle 1\rangle}$ 中有解. 证毕.

根据上面两个引理, 容易证明下面的主要定理.

定理 9.1.3 设 $f(\overline{X})$ 是域 F 上一个 n 元多项式, $n\geqslant 2$, 则方程 $f(\overline{X})=0$ 在 R 中有解, 当且仅当如下四个叙述之一成立:

(1) 方程 $f(0,x_2,\cdots,x_n)=0$ 在 R 中有解;

(2) 对于某个 $j\in\{2,\cdots,n\}$, 方程 $f(x_1,\cdots,x_{j-1},t^{-1},x_{j+1},\cdots,x_n)=0$ 在 $R_{\langle 1\rangle}$

中有解;

(3) 对于某个 $j \in \{2, \cdots, n\}$, 方程 $f(x_1, \cdots, x_{j-1}, -t^{-1}, x_{j+1}, \cdots, x_n) = 0$ 在 $R_{\langle 1\rangle}$ 中有解;

(4) 方程组

$$\begin{cases} f(\overline{X}) &= 0, \\ \dfrac{\partial f(\overline{X})}{\partial x_i} &= 0, \qquad i = 2, \cdots, n \end{cases}$$

在 R 中有解.

证明 设方程 $f(\overline{X}) = 0$ 在 R 中有解, 则 $\mathcal{V}_R(f; x_1)$ 非空. 当 $\mathcal{V}_R(f; x_1)$ 无有限端点时, 必有 $\mathcal{V}_R(f; x_1) = R$, 从而方程 $f(0, x_2, \cdots, x_n) = 0$ 在 R 中有解. 当 $\mathcal{V}_R(f; x_1)$ 具有有限端点时, 根据引理 9.1.1 和引理 9.1.2, 叙述 (2), (3) 和 (4) 中之一成立.

反过来, 若叙述 (2) 或 (3) 成立, 则下列语句在 $R_{\langle 1\rangle}$ 中成立:

$$\exists(x_1, \cdots, x_n)\big(f(x_1, \cdots, x_n) = 0\big).$$

由于上面语句中的常量 (即多项式 $f(\overline{X})$ 的系数) 都在 R 中, 从而由转移定理知, 上面语句在 R 中也成立, 即方程 $f(\overline{X}) = 0$ 在 R 中有解. 此外, 由叙述 (1) 或 (4) 显然可知, 方程 $f(\overline{X}) = 0$ 在 R 中有解. 证毕.

当 $n = 2$ 时, 由上面的定理, 立即可以获得下面结论.

推论 设 $f(x, y) \in F[x, y]$, 则方程 $f(x, y) = 0$ 在 R 中有解, 当且仅当如下四个叙述之一成立:

(1) 方程 $f(0, y) = 0$ 在 R 中有解;

(2) 方程 $f(x, t^{-1}) = 0$ 在 $R_{\langle 1\rangle}$ 中有解;

(3) 方程 $f(x, -t^{-1}) = 0$ 在 $R_{\langle 1\rangle}$ 中有解;

(4) 方程组: $f(x, y) = 0$, $\dfrac{\partial f(x, y)}{\partial y} = 0$ 在 R 中有解.

类似地, 我们可以建立下面的定理 9.1.4 及其推论. 这些结论是定理 9.1.3 及其推论的一种变形, 它们在处理对称多项式时特别适用.

定理 9.1.4 设 $f(\overline{X})$ 是域 F 上一个 n 元多项式, $n \geqslant 2$, 则方程 $f(\overline{X}) = 0$ 在 R 中有解, 当且仅当如下四个叙述之一成立:

(1) 方程 $f(t^{-1}, x_2, \cdots, x_n) = 0$ 在 $R_{\langle 1\rangle}$ 中有解;

(2) 对于某个 $j \in \{2, \cdots, n\}$, 方程 $f(x_1, \cdots, x_{j-1}, t^{-1}, x_{j+1}, \cdots, x_n) = 0$ 在 $R_{\langle 1\rangle}$ 中有解;

(3) 对于某个 $j \in \{2, \cdots, n\}$, 方程 $f(x_1, \cdots, x_{j-1}, -t^{-1}, x_{j+1}, \cdots, x_n) = 0$ 在 $R_{\langle 1\rangle}$ 中有解;

(4) 方程组

$$\begin{cases} f(\overline{X}) = 0\,, \\ \dfrac{\partial f(\overline{X})}{\partial x_i} = 0, \qquad i = 2, \cdots, n \end{cases}$$

在 R 中有解.

推论 设 $f(x,y) \in F[x,y]$, 则方程 $f(x,y)=0$ 在 R 中有解, 当且仅当如下四个叙述之一成立:

(1) 方程 $f(t^{-1},y)=0$ 在 $R_{\langle 1\rangle}$ 中有解;

(2) 方程 $f(x,t^{-1})=0$ 在 $R_{\langle 1\rangle}$ 中有解;

(3) 方程 $f(x,-t^{-1})=0$ 在 $R_{\langle 1\rangle}$ 中有解;

(4) 方程组: $f(x,y)=0, \dfrac{\partial f(x,y)}{\partial y}=0$ 在 R 中有解.

在下面, 我们将应用上面的结果给出一些有效算法, 用来判定 F 上二元多项式是否在 R 中有解 (等价于: 正定) 或者半定. 注意到: "去重因式" 不影响多项式的解集, "去偶次重因式" 不影响多项式的半定性, 同时这两种运算过程都是有效的, 且所产生的结果都是无重因式多项式. 因此, 在下文中, 不妨直接考虑无重因式的多项式.

对于 $F[x,y]$ 中一个无重因式多项式 $f(x,y)$, 总可通过 "求最大公因式" 的有效方法, 将 $f(x,y)$ 表为 $f(x,y)=h(x)g(x,y)$, 其中 $h(x)\in F[x]$, 且 $g(x,y)$ 是在 $F[x]$ 上含 y 的本原多项式 (即 $x-$ 本原多项式). 显然, $f(x,y)$ 有实零点, 当且仅当 $h(x)$ 或 $g(x,y)$ 有实零点. 同时易知, $f(x,y)$ 是半定的, 当且仅当 $h(x)$ 在 R 中无零点且 $g(x,y)$ 是半定的. 因此, 我们只需考虑无重因式的 $x-$ 本原多项式.

设 $f(x,y)$ 是 $F[x,y]$ 中一个无重因式的 $x-$ 本原多项式, 令 $g=\dfrac{\partial f(x,y)}{\partial y}$, 且 $\mathrm{Id}(f,g)$ 表示 $F[x,y]$ 中由 f 和 g 生成的理想. 记 $\mathrm{Res}(f,g;x)$, $\mathrm{Res}(f,g;y)$ 分别是 f 和 g 关于变元 x, y 的结式. 由结式的一个熟知结果 (见文献 [137] 中引理 7.2.1), $\mathrm{Res}(f,g;x)$, $\mathrm{Res}(f,g;y)\in \mathrm{Id}(f,g)$. 假若 $\mathrm{Res}(f,g;x)=0$, 则 f 和 g 有非常量公因式, 从而有公共的不可约因式 p. 由于 $f(x,y)$ 是 $x-$ 本原的, 从而 p 中必含变元 y. 又由于 g 是 f 关于变量 y 的偏导数, 从而 p 是 f 的重因式, 矛盾. 同样可证, $\mathrm{Res}(f,g;y)\neq 0$. 设 $u(x)$, $v(y)$ 分别是 $\mathrm{Res}(f,g;y)$, $\mathrm{Res}(f,g;x)$ 的无重因式部分. 由文献 [22] 中引理 8.13 易知, $\mathrm{Id}(f,g,u(x),v(y))$ 是 $F[x,y]$ 中一个维数 $\leqslant 0$ 的根理想, 且 $\mathrm{Id}(f,g,u(x),v(y))$ 的维数为零, 当且仅当 $u(x)$ 和 $v(y)$ 都不是 F 中常量.

现设 $u(x)$, $v(y)\notin F$, 即根理想 $\mathrm{Id}(f,g,u(x),v(y))$ 的维数为零. 由文献 [22] 中命题 6.77 和定理 8.81 知, 通过有限次测试, 必可获得某个 $e\in F$(甚至可取 e 为整数), 使得通过变换: $y\longmapsto y-ex$ 后, 理想 $\mathrm{Id}(f,g,u(x),v(y))$ 处于正规位置, 且其关于字典序: $y\prec x$ 的简化 Gröbner 基 具有如下形式:

$$\{x - w(y),\ h(y)\},$$

这里 $w(y), h(y) \in f[y]$.

定理 9.1.5 设多项式 $f(x,y), g(x,y), u(x), v(y)$ 和 $h(y)$ 同上, 则方程 $f(x,y) = 0$ 在 R 中有解, 当且仅当下面四个叙述之一成立:

(1) 一元方程 $f(0,y) = 0$ 在 R 中有解;

(2) 一元方程 $f(x,t^{-1}) = 0$ 在 $R_{\langle 1\rangle}$ 中有解;

(3) 一元方程 $f(x,-t^{-1}) = 0$ 在 $R_{\langle 1\rangle}$ 中有解;

(4) $u(x), v(y) \notin F$, 且一元方程 $h(y)$ 在 R 中有解.

证明 只需证明, 定理 9.1.3 的推论中的叙述 (4) 等价于定理中的叙述 (4). 由结式的另一个熟知事实知, 理想 $\mathrm{Id}(f,g)$ 和 $\mathrm{Id}(f,g,u(x),v(y))$ 在 R 中有相同的零点集. 再由 Gröbner 基 的定义, 显然 $\mathrm{Id}(f,g,u(x),v(y))$ 在 R 中的零点集与 $\mathrm{Id}(x-w(y),h(y))$ 在 R 中的零点集是一一对应的, 而后者由方程 $h(y)=0$ 在 R 中的解惟一确定. 证毕.

注 在上面的讨论中, 若结式 $\mathrm{Res}(f,g;x)$ 和 $\mathrm{Res}(f,g;y)$ 都无重因式, 则有 $\mathrm{Id}(f,g) = \mathrm{Id}(f,g,u(x),v(y))$. 从而 $\mathrm{Id}(f,g)$ 是 $F[x,y]$ 中维数 $\leqslant 0$ 的根理想.

作为定理 9.1.5 的一个应用, 我们来处理下面的实例.

例 1 确定方程 $f(x,y) = 0$ 是否有实解, 这里 $f(x,y) = x^2y^2 + x^2 - xy + y^4 - y^2 + 1$.

计算过程 (1) 考虑多项式 $f(0,y) = y^4 - y^2 + 1$, 易知它无实零点.

(2) 考虑多项式 $f(x,t^{-1}) = (1+t^{-2})x^2 - t^{-1}x + (t^{-4} - t^{-2} + 1)$. 这是一元二次多项式, 其判别式为: $\Delta = (-t^{-1})^2 - 4(1+t^{-2})(t^{-4} - t^{-2} + 1)$. 注意到, Δ 作为含 t^{-1} 的多项式, 其首项系数为 -4, 且 t^{-1} 在有理数域上是无限大正元素. 从而 $\Delta < 0$. 因此, $f(x,t^{-1})$ 无实零点.

(3) 类似于过程 (2) 可知, $f(x,-t^{-1})$ 无实零点.

(4) 计算 $g := \dfrac{\partial f(x,y)}{\partial y} = 2x^2y - x + 4y^3 - 2y$. 经检验, $\mathrm{Res}(f,g;x)$ 和 $\mathrm{Res}(f,g;y)$ 都无重因式. 通过计算得, 理想 $\mathrm{Id}(f,g)$ 关于字典序: $y \prec x$ 的简化 Gröbner 基为

$$\{2x - 4y^9 - 20y^7 - 23y^5 + 17y^3 + 9y,\ h(y)\},$$

其中 $h(y) = 4y^{10} + 16y^8 + 3y^6 - 36y^4 + 16y^2 + 1$. 借助于 Sturm 定理可知, 多项式 $h(y)$ 无实根.

根据定理 9.1.5, 所给的多项式方程 $f(x,y) = 0$ 无实解, 换句话说, $f(x,y)$ 是 (正) 定的.

至于判定多项式的半定性, 下面简单的引理表明可将问题转化为判定解的存在性.

引理 9.1.6 设 $f(\overline{X}) \in F[x_1, \cdots, x_n]$, 且它关于某一字典序的首项系数的符号为 $\epsilon(=\pm 1)$, 则 $f(\overline{X})$ 在 R 中半定, 当且仅当 $f(\overline{X})+\epsilon\eta$ 在 $R^n_{\langle n\rangle}$ 中无零点, 这里 $\eta \in R_{\langle n\rangle}$ 是 F 上的正无限小元素.

证明 设 $f(\overline{X})+\epsilon\eta$ 在 $R^n_{\langle n\rangle}$ 中有零点 $\bar{\alpha}$, 则 $f(\bar{\alpha})+\epsilon\eta=0$. 由此有 $\epsilon f(\bar{\alpha}) = -\epsilon^2\eta<0$. 由转移定理知, 存在 $\bar{a}\in R^n$, 使得 $\epsilon f(\bar{a})<0$. 注意到 $\epsilon f(x)$ 的首项系数为正, 从而必存在 $\bar{b}\in R^n$, 使得 $\epsilon f(\bar{b})>0$. 这表明: $f(\overline{X})$ 在 R 中不是半定的.

反过来, 设 $f(\overline{X})$ 在 R 中不是半定的, 则存在 $\bar{a}, \bar{b}\in R^n$, 使得 $f(\bar{a})<0$, 但 $f(\bar{b})>0$. 从而有 $f(\bar{a})+\epsilon\eta<0$, 但 $f(\bar{b})+\epsilon\eta>0$. 由实闭域 $R_{\langle n\rangle}$ 上的中间值定理, $f(\overline{X})+\epsilon\eta$ 在 $R^n_{\langle n\rangle}$ 中有零点.

由引理 9.1.6, 容易建立下面的结论. 证毕.

定理 9.1.7 设 $f(x,y)$ 同定理 9.1.5, 且 ϵ 是 $f(x,y)$ 关于某个字典序的首项系数的符号, 则 $f(x,y)$ 在 R 中半定, 当且仅当下面四个叙述都成立:

(1) $f(0,y)$ 在 R 中的每个根具有偶重数 (即 $f(0,y)$ 在 R 中是半定的);

(2) 方程 $f(x,t^{-1})=0$ 在 $R_{\langle 1\rangle}$ 中无解;

(3) 方程 $f(x,-t^{-1})=0$ 在 $R_{\langle 1\rangle}$ 中无解;

(4) 方程组: $f(x,y)+\epsilon t=0, \dfrac{\partial f(x,y)}{\partial y}=0$ 在 $R_{\langle 1\rangle}$ 中无解.

证明 不妨设 $\epsilon=1$, 且记 $f_1(x,y):=f(x,y)+t\in R_{\langle 1\rangle}[x,y]$.

设 $f(x,y)$ 在 R 中是半定的. 显然, $f(0,y)$ 在 R 中也是半定, 从而有叙述 (1). 再由转移定理知, $f(x,t^{-1})$ 和 $f(x,-t^{-1})$ 在 $R_{\langle 1\rangle}$ 中都是半定的. 由所设知, $f(x,t^{-1})$ 和 $f_1(x,-t^{-1})$ 作为 $R_{\langle 1\rangle}[x]$ 中多项式都没有重因式. 此时易知, 叙述 (2) 和 (3) 都成立. 此外, 由引理 9.1.6 知, $f_1(x,y)$ 在 $R_{\langle 1\rangle}$ 中无零点. 从而叙述 (4) 显然成立.

反过来, 设上面四个叙述都成立. 由转移定理和叙述 (2) 可知, $f(x,t^{-1})$ 在 $R_{\langle 2\rangle}$ 中也无零点. 注意到子域 $F(t_2)$ 序同构于 $F(t)$, 从而可知, $f(x,t_2^{-1})$ 在 $R_{\langle 2\rangle}$ 中无零点. 于是 $f(t_2^{-1},t^{-1})$ 与 $f(1,t^{-1})$ 同号, 而 $f(t^{-1},t_2^{-1})$ 与 $f(1,t_2^{-1})$ 同号. 由于 $f(1,t^{-1})$ 与 $f(1,t_2^{-1})$ 同号, 从而 $f(t_2^{-1},t^{-1})$ 与 $f(t^{-1},t_2^{-1})$ 有相同符号. 由 $F_{\langle 2\rangle}$ 的序结构知, $f(t_2^{-1},t^{-1})$ 与 $f(t^{-1},t_2^{-1})$ 中总有一个的符号为 $+$. 从而可知, $f(x,t^{-1})$ 与 $f(x,t_2^{-1})$ 都是正定的. 于是 $f(x,t_2^{-1})+t$ 即 $f_1(x,t_2^{-1})$ 在 $R_{\langle 2\rangle}$ 中无零点.

由叙述 (1) 知, $f(0,y)$ 在 R 中是半定的. 由上面讨论, $f(x,t^{-1})$ 是正定的. 从而 $f(0,t^{-1})>0$. 于是 $f(0,y)$ 是半正定的. 从而 $f(0,y)+t$ 即 $f_1(0,y)$ 在 $R_{\langle 1\rangle}$ 中无零点.

又由于 $f(0,y)$ 是半正定的, 从而 $f(0,-t^{-1})\geqslant 0$. 再由叙述 (3) 即知, $f(x,-t^{-1})$ 是正定的. 同样可知, $f(x,-t_2^{-1})$ 也是正定的. 从而 $f(x,-t_2^{-1})+t$ 即 $f_1(x,-t_2^{-1})$ 在 $R_{\langle 2\rangle}$ 中无零点.

再由叙述 (4) 知，方程组 $f_1(x,y)=0,\ \dfrac{\partial f_1(x,y)}{\partial y}=0$ 在 $R_{\langle 1\rangle}$ 中无解. 注意到，t_2 是 $F_{\langle 1\rangle}$ 上的无限小正元素. 根据定理 9.1.3 的推论知，方程 $f_1(x,y)=0$ 在 $R_{\langle 1\rangle}$ 中无解. 最后，由引理 9.1.6 知，$f(x,y)$ 在 R 中是半定的. 证毕.

作为定理 9.1.7 的一个应用，我们处理下面的实例.

例 2 判定多项式 $f(x,y)$ 是否半定，这里 $f(x,y)=x^4+x^2y^2+2y^4-4xy+1$.

计算过程 (1) 考虑多项式 $f(0,y)=2y^4+1$, 易知它无实零点.

(2) 计算多项式 $f(x,t^{-1})$ 的 Sylvester 矩阵的偶次顺序主子式如下：

$$4,\ -8t^{-2},\ 56t^{-6}-544t^{-2},\ 1568t^{-12}+7120t^{-8}-3200t^{-4}+256.$$

上面序列的 (修订) 变号数为 2. 由定理 2.5.4 知，$f(x,t^{-1})$ 无实零点.

(3) 类似于过程 (2) 可知，$f(x,-t^{-1})$ 无实零点.

(4) 令 $g:=\dfrac{\partial f(x,y)}{\partial y}$. 经检验，$\mathrm{Res}(f+t,g;x)$ 和 $\mathrm{Res}(f+t,g;y)$ 都无重因式. 计算理想 $\mathrm{Id}(f+t,g)$ 关于字典序 $y\prec x$ 的简化 Gröbner 基为

$$\{(72t-632)x+1764y^{11}+(4132+252t)y^7+(861-538t+9t^2)y^3,\ h(y)\},$$

其中 $h(y)=196y^{12}+(372+28t)y^8+(t^2-66t-163)y^4+(16+16t)$.

这表明理想 $\mathrm{Id}(f+t,g)$ 关于变量 y 处于正规位置. 从而方程组 $f+t=0,\ g=0$ 有实解，当且仅当多项式 $h(y)$ 有实零点. 显然，这又相当于下面多项式 h_1 有实零点：

$$h_1(y)=196y^6+(372+28t)y^4+(t^2-66t-163)y^2+(16+16t).$$

计算多项式 h_1 的 Sylvester 矩阵的偶次顺序主子式，获得该序列的符号表如下：

$$1,\ -1,\ -1,\ -1,\ -1,\ -1.$$

上面符号表的 (修订) 变号数为 1. 由定理 2.5.4 知，$h_1(y)$ 的实零点个数为 $6-2\times 1=4$. 从而，方程组 $f+t=0,\ g=0$ 有实解.

根据定理 9.1.7 知，所给的多项式 $f(x,y)$ 是不定的.

§9.2 半定多项式的有效判定

判定多项式的半定性这一问题涉及到许多领域, 例如有序几何中的自动推理、不等式的研究和多项式理想的实根计算. 在本节中, 我们将给出一个判定系数在可计算序域中的多项式的半定性的有效方法, 如果这序域容纳一个有效算法, 使得每

个非零单元多项式的全部实零点都能找到隔离点. 基于我们的方法, 半定多元多项式的判定可以简化为对一些含较少变量的多项式的测试, 其中被简化的多项式的全次数和项数都不超过所给的多项式.

设 $(F,\leqslant)$ 是一个实闭包为 R 的可计算序域. 对于一个在 R 中有零点的非零单元多项式 $f(x)\in F[x]$, F 的一个有限子集 Γ 称作 $f(x)$ 的一个隔离集, 如果下列条件成立: (1) 对于每个 $a\in\Gamma$, $f(a)\neq 0$; (2) 对于 $f(x)$ 在 R 中的每个零点 α, 存在 $a,b\in\Gamma$, 其中 $a<b$, 使得开区间 $]a,b[$ 仅包含 $f(x)$ 在 R 中的这个零点 α. 为方便起见, 对于每个在 R 中无零点的非零多项式 $f(x)\in F[x]$, 规定 $\{0\}$ 是它惟一的隔离集. 这样, 任意非零单元多项式的每个隔离集都是非空的. 根据文献 [22] 中定理 8.115, 有理数域 $\mathbb{Q}$ 容纳一个寻找非零单元多项式的隔离集的有效方法. 因此, 我们的结论适用于 $\mathbb{Q}$ 上半正定多项式的测试. 为了提高计算效率, 著名的吴方法 在本节中起着重大作用.

在建立主要结论之前, 我们需要一些有关的引理. 设 A 是 F 的代数闭包, 且 $F[\overline{X}]:=F[x_1,\cdots,x_n]$ 是域 F 上含未定元 $x_1,\cdots,x_n$ 的多项式环. 对于 $f\in F[\overline{X}]$, f 被称作非奇异的, 如果方程组 $f=0$, $\dfrac{\partial f}{\partial x_i}=0, i=1,\cdots,n$ 在 A 中无解. 由熟知的 Hilbert 零点定理可知, $F[\overline{X}]$ 中多项式 f 是非奇异的, 当且仅当 $1\in I$, 其中 I 是 $F[\overline{X}]$ 中由 f 和 $\dfrac{\partial f}{\partial x_i}=0, i=1,\cdots,n$, 生成的理想.

引理 9.2.1 设 $f(x_1,x_2,\cdots,x_n)\in F[\overline{X}]$ 是非奇异的, 且 I 是 $F[\overline{X}]$ 中由 f 和 $\dfrac{\partial f}{\partial x_i}, i=1,\cdots,n-1$, 生成的理想, 则 $I\cap F[x_n]\neq\{0\}$.

证明 令 $\mathcal{V}_A(f)$ 表示 f 在 A^n 中的簇 (零点集), 则我们有一个从 $\mathcal{V}_A(f)$ 到仿射空间 A 中的正则映射 π, 使得 $\pi(y_1,\cdots,y_n)=y_n$, 对于每个 $(y_1,\cdots,y_n)\in\mathcal{V}_A(f)$. 设 $\mathcal{W}$ 是 $\pi(\mathcal{V}_A(f))$ 关于 A 的 Zariski 拓扑的闭包. 由 Bertini 第二定理 (见 [181], 第 II 章 §6 中定理 2), 存在一个稠密的开集 $\mathcal{O}\subseteq\mathcal{W}$, 使得对于每个 $y\in\mathcal{O}$, $\pi^{-1}(y)$ 是非奇异的. 此时, $\mathcal{W}\setminus\mathcal{O}$ 对于 Zariski 拓扑是 A 的一个闭子集, 且 $\mathcal{W}\setminus\mathcal{O}\neq A$. 根据 A 中闭子集的构造 (参见 [181], 第 23 页的例 3), $\mathcal{W}\setminus\mathcal{O}=\mathcal{V}_A(g)$, 其中 $g(x_n)\in F[x_n]$ 是一个非零的单元多项式.

注意到, $\pi(\mathcal{V}_A(I))\cap\mathcal{O}=\phi$, 这里 $\mathcal{V}_A(I)$ 是 I 在 A^n 中的簇; 否则存在一个 $y'\in\pi(\mathcal{V}_A(I))\cap\mathcal{O}$, 使得 $\pi^{-1}(y')$ 是非奇异的. 这样, 我们有 $\pi(\mathcal{V}_A(I))\subseteq\mathcal{W}\setminus\mathcal{O}$. 这表明: $g(y_n)=0$, 对于所有 $(y_1,\cdots,y_n)\in\mathcal{V}_A(I)$. 由 Hilbert 零点定理知, 有某个正整数 s, 使得 $g^s\in I$. 显然, $g^s\in I\cap F[x_n]$. 证毕.

注意到, 对于所有 $f\in F[\overline{X}]$, $z-f\in F[\overline{X},z]$ 是非奇异的. 从而, 我们可以建立下面的一个直接推论.

推论 设 $f(x_1,x_2,\cdots,x_n)\in F[\overline{X}]$, 且 I 是 $F[\overline{X},z]$ 中由 $z-f$ 和 $\dfrac{\partial f}{\partial x_i}, i=1,\cdots,n$, 生成的理想, 则 $I\cap F[z]\neq\{0\}$.

现设 f 是 $F[\overline{X}]$ 中一个正次数多项式，且记 $\mathcal{S}_R(f,x_n) := \{a_n \in R \mid 有\ a_1, \cdots, a_{n-1} \in R\ 使得\ f(a_1,a_2,\cdots,a_n) < 0\}$. 由文献 [25] 中命题 2.1.7 知，当多项式 $f(\overline{X})$ 在 R 上不是半正定时，$\mathcal{S}_R(f,x_n)$ 是由 R 中有限个不相交的开区间所组成. 显然，当 $\mathcal{S}_R(f,x_n) \neq R$ 时，$\mathcal{S}_R(f,x_n)$ 至少有一个有限端点. 我们的目的是寻求一个有效方法以判定 $\mathcal{S}_R(f,x_n)$ 中有限端点的存在，这里 f 是 $F[\overline{X}]$ 中一个不定多项式. 为此目的，我们将按照 §9.1 中的方法，把原来的序域 F 扩充为一个包含无限小正元素 $\epsilon_0, \epsilon_1, \cdots, \epsilon_n$ 的可计算的非阿基米德序域.

对于一个非负整数 m, 令 $F_{\langle m\rangle} := F(\epsilon_0,\cdots,\epsilon_m)$, 其中 $\epsilon_0,\cdots,\epsilon_m$ 是 F 上 $m+1$ 个未定元. 由 §9.1 中的讨论，F 的序 $\leqslant$ 可惟一地拓展为 $F_{\langle m\rangle}$ 的一个序，仍记作 $\leqslant$, 使得 ϵ_0 是 F 上无限小正元素，同时 ϵ_k 是 $F(\epsilon_0,\cdots,\epsilon_{k-1})$ 上无限小正无素，$k=1,\cdots,m$. 同样，记 $R_{\langle m\rangle}$ 为 $(F_{\langle m\rangle},\leqslant)$ 的实闭包，且认定：$R \subset R_{\langle m\rangle}$. 对于 $k=0,\cdots,m-1$, 记 $R_{\langle k\rangle}$ 为 $F_{\langle k\rangle}$ 在 $R_{\langle m\rangle}$ 中的代数闭包，则 $R_{\langle k\rangle}$ 是 $F_{\langle k\rangle}$ 关于序 $\leqslant$ 的实闭包，且 $R \subset R_{\langle 0\rangle} \subset R_{\langle 1\rangle} \subset \cdots \subset R_{\langle m\rangle}$.

对于取定的 $n \in \mathbb{N}$, 构造 $R_{\langle n\rangle}$ 的如下两个子集:

$$A := \{z \in R_{\langle n\rangle} \mid 对于某个正元素\ d \in R,\ -d \leqslant z \leqslant d\},$$
$$M := \{z \in R_{\langle n\rangle} \mid 对于每个正元素\ d \in R,\ -d \leqslant z \leqslant d\}.$$

同样，我们可构造 $R_{\langle n\rangle}$ 的如下两个子集:

$$A_{\langle 0\rangle} := \{z \in R_{\langle n\rangle} \mid 对于某个正元素\ d \in R_{\langle 0\rangle},\ -d \leqslant z \leqslant d\},$$
$$M_{\langle 0\rangle} := \{z \in R_{\langle n\rangle} \mid 对于每个正元素\ d \in R_{\langle 0\rangle},\ -d \leqslant z \leqslant d\}.$$

显然，M 是由 $R_{\langle n\rangle}$ 中所有在 R 上无限小的元素组成，而 $M_{\langle 0\rangle}$ 是由 $R_{\langle n\rangle}$ 中所有在 $R_{\langle 0\rangle}$ 上无限小的元素组成. 根据序 $\leqslant$ 的结构，$R \subset A \subset R_{\langle n\rangle}$, $R_{\langle 0\rangle} \subset A_{\langle 0\rangle} \subset R_{\langle n\rangle}$, $\epsilon_0, \epsilon_1, \cdots, \epsilon_n \in M$, 且 $\epsilon_1, \cdots, \epsilon_n \in M_{\langle 0\rangle}$. 由实赋值的熟知结果知，$A$ 是 $R_{\langle n\rangle}$ 的一个实赋值环，其极大理想为 M, 而 $A_{\langle 0\rangle}$ 是 $R_{\langle n\rangle}$ 的另一个实赋值环，其极大理想为 $M_{\langle 0\rangle}$. 此外，A 和 $A_{\langle 0\rangle}$ 都与序 $\leqslant$ 相容. 换言之，A, M, $A_{\langle 0\rangle}$ 和 $M_{\langle 0\rangle}$ 在 $R_{\langle n\rangle}$ 中关于序 $\leqslant$ 都是凸的. 注意到，剩余域 A/M 同构于 R, 而剩余域 $A_{\langle 0\rangle}/M_{\langle 0\rangle}$ 同构于 $R_{\langle 0\rangle}$. 从而存在一个从 A 到 R 的同态 π, 使得对于每个 $f \in R[\epsilon_0,\cdots,\epsilon_n]$, $\pi(f(\epsilon_0,\cdots,\epsilon_n)) = f(0,\cdots,0)$. 并且存在一个从 $A_{\langle 0\rangle}$ 到 $R_{\langle 0\rangle}$ 的同态 π_0, 使得对于每个 $g \in R_{\langle 0\rangle}[\epsilon_1,\cdots,\epsilon_n]$, $\pi_0(g(\epsilon_1,\cdots,\epsilon_n)) = g(0,\cdots,0)$.

对于每个 $g \in F_{\langle 0\rangle}[\overline{X}]$, 显然 $g \in F_{\langle k\rangle}[\overline{X}]$, $k=1,\cdots,n$. 对于 $k=0,1,\cdots,n$, 用 $\mathcal{V}_{R_{\langle k\rangle}}(g,x_n)$ 表示 $R_{\langle k\rangle}$ 的如下子集:

$$\{a_n \in R_{\langle k\rangle} \mid 有\ a_1,\cdots,a_{n-1} \in R_{\langle k\rangle},\ 使得\ g(a_1,a_2,\cdots,a_n) = 0\}.$$

由文献 [25] 中命题 2.1.7 知，当多项式 g 在 $R_{\langle k\rangle}$ 中有零点时，$\mathcal{V}_{R_{\langle k\rangle}}(g,x_n)$ 是

由 $R_{\langle k\rangle}$ 中有限个不相交的 (开，闭或半开半闭) 区间所组成，这里 $\mathcal{V}_{R_{\langle k\rangle}}(g,x_n)$ 的孤立点看作左右端点相同的闭区间.

对于每个非零的 $f\in F[\overline{X}]$, 令 $f_+:=f+\epsilon_0$, 则 $f_+\in F_{\langle 0\rangle}[\overline{X}]$. 根据引理 9.1.6 及其证明，立即有这样一个事实： $\mathcal{S}_R(f,x_n)\neq\varnothing$ 当且仅当 $\mathcal{V}_{R_{\langle 0\rangle}}(f_+,x_n)\neq\varnothing$.

引理 9.2.2 设记号同上，且 I 是 $F[t,\overline{X}]$ 中由 $f+t$ 和 $\dfrac{\partial f}{\partial x_i}$, $i=1,\cdots,k$, 生成的理想，其中 t 是另一变量，且 $0\leqslant k\leqslant n-1$, 则我们有

(1) $I\cap F[t,x_{k+1},\cdots,x_n]\neq\{0\}$;

(2) 若 a_n^* 是如下集合的一个有限闭端点：

$$\mathcal{V}_{R_{\langle n-k-1\rangle}}(f_+(x_1,\cdots,x_k,\varrho_1\epsilon_1^{-1},\cdots,\varrho_{n-k-1}\epsilon_{n-k-1}^{-1},x_n),x_n),$$

$\varrho_i=\pm1$, $i=1,\cdots,n-k-1$, 则对于任意非零多项式 $g(t,x_{k+1},\cdots,x_n)\in I\cap F[t,x_{k+1},\cdots,x_n]$,

$$g(\epsilon_0,\varrho_1\epsilon_1^{-1},\cdots,\varrho_{n-k-1}\epsilon_{n-k-1}^{-1},a_n^*)=0.$$

证明 (1) 用 I^e 表示 I 在 $F(x_{k+1},\cdots,x_n)[x_1,\cdots,x_k,t]$ 中的扩理想. 由引理 9.2.1 的推论， $I^e\cap F(x_{k+1},\cdots,x_n)[t]\neq\{0\}$. 从而必有 $I\cap F[t,x_{k+1},\cdots,x_n]\neq\{0\}$.

(2) 记 $h:=f_+(x_1,\cdots,x_k,\varrho_1\epsilon_1^{-1},\cdots,\varrho_{n-k-1}\epsilon_{n-k-1}^{-1},x_n)$. 显然， h 是多项式环 $F_{\langle n-k-1\rangle}[x_1,\cdots,x_k,x_n]$ 中一个非零多项式. 设 a_n^* 是 $\mathcal{V}_{R_{\langle n-k-1\rangle}}(h,x_n)$ 的一个有限闭端点. 由引理 9.1.1 知，方程组： $h=0$, $\dfrac{\partial h}{\partial x_i}=0$, $i=1,\cdots,k$, 在 $R^n_{\langle n-k-1\rangle}$ 中有一个解 $(a_1^*,\cdots,a_k^*,a_n^*)$. 这意味着： $(\epsilon_0,a_1^*,\cdots,a_k^*,\varrho_1\epsilon_1^{-1},\cdots,\varrho_{n-k-1}\epsilon_{n-k-1}^{-1},a_n^*)$ 是 I 的一个零点. 因此，叙述 (2) 获证.

引理 9.2.3 设记号同上，且 $e(x_n)\in F[x_n]$ 是 f 作为 $F(x_n)[x_1,\cdots,x_{n-1}]$ 中多项式关于字典序 $x_1\prec\cdots\prec x_{n-1}$ 的首项系数. 如果 a 是 $\mathcal{S}_R(f,x_n)$ 的一个有限开端点，则 $e(a)=0$, 或者有 $\mathcal{V}_{R_{\langle 0\rangle}}(f_+,x_n)$ 的一个有限端点 a^*, 使得 $\pi(a^*)=a$, 即 a^*-a 在 R 上是无限小.

证明 不失一般性，我们可假定， a 是 $\mathcal{S}_R(f,x_n)$ 的一个左侧有限开端点，使得 $e(a)\neq0$. 此时，有开区间 $]a,c[\subseteq\mathcal{S}_R(f,x_n)$, 其中 $c\in R$ 且 $a<c$. 此外， $e(a)>0$; 否则 $a\in\mathcal{S}_R(f,x_n)$. 由于 R 上每个多项式函数是连续的，从而 R 中有正元素 δ, 使得对于所有 $a_n\in]a,a+2\delta[$, $e(a_n)>0$. 由于 δ 可取充分小元素，从而可认定 $[a+\delta,a+2\delta]\subseteq]a,c[$, 其中 $[a+\delta,a+2\delta]$ 是 R 中具有端点 $a+\delta$, $a+2\delta$ 的闭区间.

记 $[a+\delta,a+2\delta]_{R_{\langle 0\rangle}}$ 为 $R_{\langle 0\rangle}$ 中具有端点 $a+\delta$, $a+2\delta$ 的闭区间. 设 $a_n^*\in[a+\delta,a+2\delta]_{R_{\langle 0\rangle}}$, 则 $a_n^*\in A$, 因为 $R\subseteq A$ 且 A 在 $R_{\langle 0\rangle}$ 中是凸的. 令 $a_n:=\pi(a_n^*)$, 我们有 $a_n\in R$. 注意到 $\pi(a_n-a_n^*)=0$, 即 $a_n-a_n^*\in M$. 从而对于 R 中任意正元素 d, $-d+a+\delta<(a_n-a_n^*)+a_n^*<d+a+2\delta$, 即有 $-d+a+\delta<a_n<d+a+2\delta$.

由 d 的任意性，我们有 $a_n \in [a+\delta, a+2\delta]$. 于是 $f(x_1, \cdots, x_{n-2}, a_n)$ 在 R 上不是半正定的. 因此，有 $(a_1, \cdots, a_{n-1}) \in R^{n-1}$, 使得 $f(a_1, \cdots, a_{n-1}, a_n) < 0$. 注意到，$f(x_1, \cdots, x_{n-1}, a_n)$ 的首项系数 $e(a_n)$ 为正. 从而有某个 $(b_1, \cdots, b_{n-1}) \in R^{n-1}$, 使得 $f(b_1, \cdots, b_{n-1}, a_n) > 0$. 注意到 $f(a_1, \cdots, a_{n-1}, a_n^*) - f(a_1, \cdots, a_{n-1}, a_n) + \epsilon_0 \in M$, 因为 $\pi(f(a_1, \cdots, a_{n-1}, a_n^*) - f(a_1, \cdots, a_{n-1}, a_n) + \epsilon_0) = 0$. 从而 $f(a_1, \cdots, a_{n-1}, a_n^*) - f(a_1, \cdots, a_{n-1}, a_n) + \epsilon_0 < -f(a_1, \cdots, a_{n-1}, a_n)$, 即 $f(a_1, \cdots, a_{n-1}, a_n^*) + \epsilon_0 < 0$. 同理，$f(b_1, \cdots, b_{n-1}, a_n^*) + \epsilon_0 > 0$. 由实闭域上多项式的中间值定理，我们有 $a_n^* \in \mathcal{V}_{R_{\langle 0\rangle}}(f_+, x_n)$. 这表明，$[a+\delta, a+2\delta]_{R_{\langle 0\rangle}} \subseteq \mathcal{V}_{R_{\langle 0\rangle}}(f_+, x_n)$. 因而，对于 $\mathcal{V}_{R_{\langle 0\rangle}}(f_+, x_n)$ 的某个区间 Ω, $[a+\delta, a+2\delta]_{R_{\langle 0\rangle}} \subseteq \Omega$. 记 a^* 为 Ω 的左端点，则 $a^* < a+\delta$. 假若 $a^* < a$, 则 $a \in \mathcal{V}_{R_{\langle 0\rangle}}(f_+, x_n)$, 即对于某个 $(d_1^*, \cdots, d_{n-1}^*) \in R_{\langle 0\rangle}^{n-1}$, $f_+(d_1^*, \cdots, d_{n-1}^*, a) = 0$. 这样，我们有 $f(d_1^*, \cdots, d_{n-1}^*, a) = -\epsilon_0 < 0$. 由转移定理知，对于某个 $(d_1, \cdots, d_{n-1}) \in R^{n-1}$, $f(d_1, \cdots, d_{n-1}, a) < 0$. 这导致出矛盾：$a \in \mathcal{S}_R(f, x_n)$. 于是 $a \leqslant a^* \leqslant a+\delta$, 即 $0 \leqslant a^* - a \leqslant \delta$. 由于 δ 可取任意充分小元素，从而 $a^* - a \in M$. 因而 $\pi(a^* - a) = 0$, 即 $\pi(a^*) = a$. 证毕.

引理 9.2.4 设记号同上，且 $g(\overline{X}) \in F_{\langle 0\rangle}[\overline{X}]$. 若 a 是 $\mathcal{V}_{R_{\langle 0\rangle}}(g, x_n)$ 的一个有限开端点，则对于某个整数组 $(j_1, \cdots, j_k)$, 其中 $1 \leqslant j_1 < \cdots < j_k \leqslant n-1$, 以及某些 $\varrho_1, \cdots, \varrho_k \in \{1, -1\}$, $\mathcal{V}_{R_{\langle k\rangle}}(h, x_n)$ 有一个闭端点 a^*, 使得 $\pi_0(a^*) = a$, 这里 h 是 $F_{\langle k\rangle}$ 上这样一个多项式，它是在多项式 g 中通过代换 $x_{j_i} = \varrho_i \epsilon_i^{-1}$, $i = 1, \cdots, k$, 而获得的.

证明 不失一般性，可设 a 是 $\mathcal{V}_{R_{\langle 0\rangle}}(g, x_n)$ 的一个左侧有限开端点. 显然 $a \notin \mathcal{V}_{R_{\langle 0\rangle}}(g, x_n)$, 并且有一个 $c \in R_{\langle 0\rangle}$, 使得 $a < c$ 且 $]a, c[_{R_{\langle 0\rangle}} \subseteq \mathcal{V}_{R_{\langle 0\rangle}}(g, x_n)$. 对于每个 $\delta \in R_{\langle 0\rangle}$, 其中 $0 < \delta < c - a$, 以及每个 $i \in \{1, \cdots, n-1\}$, 构造 $R_{\langle 0\rangle}$ 的如下子集：

$$\begin{aligned} & \mathcal{W}_{\delta,i}(g; a) \\ = \ & \{z_i \in R_{\langle 0\rangle} \mid \text{存在} a_1, \cdots, a_{i-1}, a_{i+1}, \cdots, a_n \in R_{\langle 0\rangle} \\ & \text{使得} a < a_n < a+\delta, \ \text{且} g(a_1, \cdots, a_{i-1}, z_i, a_{i+1}, \cdots, a_n) = 0\}. \end{aligned}$$

为方便起见，我们称变量 x_i 在 $x_n \to a$ 时关于 g 是有界的，如果对于某个 $\delta \in R_{\langle 0\rangle}$, 其中 $0 < \delta < c - a$, $\mathcal{W}_{\delta,i}(g; a)$ 是 $R_{\langle 0\rangle}$ 的一个有界的子集. 此时，可断言：存在一个 $j \in \{1, \cdots, n-1\}$, 使得 x_j 在 $x_n \to a$ 时关于 g 不是有界的. 事实上，如若不然，则有 δ, $D \in R_{\langle 0\rangle}$, 其中 $0 < \delta < c - a$ 且 $0 < D$, 使得对于所有 $z \in \bigcup_{i=1}^{n-1} \mathcal{W}_{\delta,i}(g; a)$, 恒有 $-D < z < D$. 从而下面语句在 $R_{\langle 0\rangle}$ 中成立：

$$\forall (x_1, \cdots, x_n)\Big(g(x_1, \cdots, x_n) = 0 \wedge a < x_n < a+\delta \Longrightarrow \bigwedge_{i=1}^{n-1}(-D < x_i < D)\Big).$$

很清楚，$]a, a+\delta[_{R_{\langle 0\rangle}} \subseteq \mathcal{V}_{R_{\langle 0\rangle}}(g, x_n)$. 因而，下面语句在 $R_{\langle 0\rangle}$ 中也成立：

$$\forall x_n\Big(a < x_n < a+\delta \Longrightarrow \exists(x_1,\cdots,x_{n-1})\big(g(x_1,\cdots,x_{n-1},x_n)=0\big)\Big).$$

注意到 $R_{\langle 0\rangle} \subseteq R_{\langle 1\rangle}$. 由适合实闭域的转移原理，上面两个语句在 $R_{\langle 1\rangle}$ 中也成立. 令 $\alpha = a+\epsilon_1$, 则 $\alpha \in R_{\langle 1\rangle}$, 且 $a < \alpha < a+\delta$. 根据第二个语句，$\alpha \in \mathcal{V}_{R_{\langle 1\rangle}}(g,x_n)$, 即有 $\alpha_1,\cdots,\alpha_{n-1} \in R_{\langle 1\rangle}$, 使得 $g(\alpha_1,\cdots,\alpha_{n-1},\alpha)=0$. 由第一个语句有，$-D < \alpha_i < D$, $i=1,\cdots,n-1$. 因而 $\alpha_i \in A_{\langle 0\rangle}$, $i=1,\cdots,n-1$. 由此有 $g(\pi_0(\alpha_1),\cdots,\pi_0(\alpha_{n-1}),\pi_0(\alpha)) = \pi_0(g(\alpha_1,\cdots,\alpha_{n-1},\alpha))=0$, 即 $g(\pi_0(\alpha_1),\cdots,\pi_0(\alpha_{n-1}),a)=0$, 其中 $\pi_0(\alpha_i)\in R_{\langle 0\rangle}$, $i=1,\cdots,n-1$. 这意味着 $a \in \mathcal{V}_{R_{\langle 0\rangle}}(g,x_n)$, 矛盾.

选取最小自然数 j_1, 使得 x_{j_1} 在 $x_n \to a$ 时关于 g 不是有界的. 此时，下面语句在 $R_{\langle 0\rangle}$ 中成立:

$$\begin{aligned}&\forall(\delta,D)\Big(0<\delta<c-a\wedge 0<D\\ &\Longrightarrow \exists(x_1,\cdots,x_n)\big(g(x_1,\cdots,x_n)=0\wedge D^2<x_{j_1}^2\wedge a<x_n<a+\delta\big)\Big).\end{aligned}$$

同样，由转移原理知，上面语句在 $R_{\langle 1\rangle}$ 中成立. 注意到，$0<\epsilon_1<c-a$ 且 $0<\epsilon_1^{-1}$. 由上面语句知，存在 $b_1,\cdots,b_n \in R_{\langle 1\rangle}$, 使得 $g(b_1,\cdots,b_n)=0$, $\epsilon_1^{-2}<b_{j_1}^2$, 且 $a<b_n<a+\epsilon_1$. 由于 ϵ_1 是正元素，且它在 $R_{\langle 0\rangle}$ 上是无限小，从而 $\varrho_1 b_{j_1}^{-1}$ 也是在 $R_{\langle 0\rangle}$ 上的无限小正元素，其中 $\varrho_1=1$, 若 $0<b_{j_1}$; 或者 $\varrho_1=-1$, 若 $b_{j_1}<0$. 记 θ 为从 $R_{\langle 0\rangle}(b_{j_1})$ 到 $R_{\langle 0\rangle}(\epsilon_1)$ 的 $R_{\langle 0\rangle}$- 同构，使得 $\theta(b_{j_1})=\varrho_1\epsilon_1^{-1}$. 易见，$\theta$ 是保序的. 注意到，$R_{\langle 1\rangle}$ 既是 $R_{\langle 0\rangle}(b_{j_1})$ 的实闭包，又是 $R_{\langle 0\rangle}(\epsilon_1)$ 的实闭包. 因而，θ 可以拓展为 $R_{\langle 1\rangle}$ 的一个保序的自同构. 令 $a_1 := \theta(b_n)$, 且记 g_1 为在 g 中通过代换 $x_{j_1}=\varrho_1\epsilon_1^{-1}$ 所得的 $R_{\langle 1\rangle}$ 上多项式. 此时，$a_1 \in \mathcal{V}_{R_{\langle 1\rangle}}(g_1,x_n)$. 由不等式 $0<b_n-a<\epsilon_1$ 可知，b_n-a 是在 $R_{\langle 0\rangle}$ 上的无限小正元素. 从而，a_1-a 是在 $R_{\langle 0\rangle}$ 上的无限小正元素.

由 [25] 中命题 2.1.7 知，对于 $\mathcal{V}_{R_{\langle 1\rangle}}(g_1,x_n)$ 的某个区间 Ω, $a_1\in\Omega$. 用 a_1^* 表示 Ω 的左端点. 必然 $a_1^*\leqslant a_1$. 假若 $a_1^*<a$, 则 $a\in\mathcal{V}_{R_{\langle 1\rangle}}(g_1,x_n)$. 根据转移原理，我们有 $a\in\mathcal{V}_{R_{\langle 0\rangle}}(g,x_n)$, 矛盾. 因而，$a\leqslant a_1^*\leqslant a_1$. 于是，$a_1^*-a$ 是在 $R_{\langle 0\rangle}$ 上的无限小非负元素. 此外，我们可证明如下断言.

断言 关于 g_1, x_i 在 $x_n\to a_1^*$ 时是有界的，$i\in\{1,\cdots,j_1-1\}$.

事实上，由 j_1 的选取知，x_i 在 $x_n\to a$ 时关于 g 是有界的. 于是，有某两个 $\delta, D\in R_{\langle 0\rangle}$, 其中 $0<\delta<c-a$ 且 $0<D$, 使得对于所有 $z\in\bigcup_{i=1}^{j_1-1}\mathcal{W}_{\delta,i}(g;a)$, 总有 $-D<z<D$. 因而，下面语句在 $R_{\langle 0\rangle}$ 中成立:

$$\begin{aligned}\forall(x_1,\cdots,x_n)\Big(&g(x_1,\cdots,x_n)=0\wedge a<x_n<a+\delta\\ &\Longrightarrow \textstyle\bigwedge_{i=1}^{j_1-1}(-D<x_i<D)\Big).\end{aligned}$$

由转移原理，上面语句在 $R_{\langle 1\rangle}$ 中也成立. 由于 a_1^*-a 是在 $R_{\langle 0\rangle}$ 上的无限小非负元素，从而 $a\leqslant a_1^*<a_1^*+\dfrac{1}{2}\delta<a+\delta$. 由上面语句在 $R_{\langle 1\rangle}$ 中的有效性可见，对于所有 $z\in\bigcup_{i=1}^{j_1-1}\mathcal{W}_{\frac{1}{2}\delta,i}(g_1;a_1^*)$, 总有 $-D<z<D$. 因而，上面的断言获证.

若 a_1^* 是 $\mathcal{V}_{R_{\langle 1\rangle}}(g_1,x_n)$ 的一个闭端点，则引理证毕. 现设 a_1^* 是 $\mathcal{V}_{R_{\langle 1\rangle}}(g_1,x_n)$ 的一个开端点. 重复前面的讨论可知，在 $\{1,\cdots,n-1\}\setminus\{j_1\}$ 中有一个最小自然数 j_2, 使得 x_{j_2} 在 $x_n\to a_1^*$ 时关于 g_1 不是有界. 由上面断言知， $j_1<j_2$. 记 g_2 为在 g_1 中通过代换： $x_{j_2}=\varrho_2\epsilon_2^{-1}$ 所得的 $R_{\langle 2\rangle}$ 上多项式，这里 $\varrho_2=1$ 或 -1 同上而定. 类似地，我们可证明下列事实： (1) 存在 $\mathcal{V}_{R_{\langle 2\rangle}}(g_2,x_n)$ 的一个有限端点 a_2^*, 使得 $a_2^*-a_1^*$ 是在 $R_{\langle 1\rangle}$ 上的无限小非负元素，自然也是在 $R_{\langle 0\rangle}$ 上的无限小非负元素； (2) 关于 g_2, x_i 在 $x_n\to a_2^*$ 时是有界的， $i\in\{1,2,\cdots,j_2-1\}\setminus\{j_1\}$.

只要 a_2^* 是 $\mathcal{V}_{R_{\langle 2\rangle}}(g_2,x_n)$ 的开端点，关于 g_2 的讨论可类似地进行下去. 最后，在进行第 k 次讨论后，我们能够得到一个整数组 $(j_1,\cdots,j_k)$, 其中 $1\leqslant j_1<\cdots<j_k\leqslant n-1$, 以及一个序列 $a_1^*,\cdots,a_k^*$, 使得如次条件被满足： (1)a_k^* 是 $\mathcal{V}_{R_{\langle k\rangle}}(g_k,x_n)$ 的一个闭端点，这里 g_k 是在 g 中通过代换： $x_{j_i}=\varrho_i\epsilon_i^{-1}$ $(i=1,\cdots,k)$ 所得的 $F_{\langle k\rangle}$ 上多项式，其中 $\varrho_1,\cdots,\varrho_k\in\{1,-1\}$ 按前面方式而确定； (2) 全部元素 a_1^*-a, $a_2^*-a_1^*,\cdots,a_k^*-a_{k-1}^*$ 都是在 $R_{\langle 0\rangle}$ 上的无限小非负元素. 由条件 (2), a_k^*-a 是在 $R_{\langle 0\rangle}$ 上的无限小元素，从而 $\pi_0(a_k^*)=a$. 引理获证.

为了获得如引理 9.2.2 所述的 $I\cap F[t,x_{k+1},\cdots,x_n]$ 中非零多项式，著名的吴方法是一个有效工具. 作为吴方法的一个重要结果，我们引述如下定理 (参见文献 [196] 中定理 6.10):

吴定理 设 F 是一个域，且 PS 是 $F[\overline{X}]$ 中有限个多项式组成的集合，则存在一个有效方法，可构作一系列不可约升列： $PC_1,\cdots,PC_r$, 使得

$$\mathrm{Zero}(PS)=\bigcup_{1\leqslant j\leqslant r}\mathrm{Zero}(PC_j/I_j).$$

这里 I_j 是 PC_j 的初式集， $\mathrm{Zero}(PS)$ 表示 PS 在 F 的任意一个代数闭扩张中全部零点所组成的集合，而对于 $j=1,\cdots,r$, $\mathrm{Zero}(PC_j/I_j)$ 表示 PC_j 在 F 的任意一个代数闭扩张中全部这样的零点所组成的集合，这些零点不是 I_j 中任何一个成员的零点.

应该指出，对于系数为有理数的多项式，吴方法已经被编制成可生成不可约升列的计算机软件.

引理 9.2.5 设 F 是一个域， PS 是 $F[\overline{X}]$ 中有限个多项式组成的集合，且 I 是 $F[\overline{X}]$ 中由 PS 生成的理想，使得 $I\cap F[x_1,\cdots,x_r]\neq\{0\}$, 其中 $1\leqslant r\leqslant n$. 如果 $PC_1,\cdots,PC_r$ 是 PS 关于字典序 $x_1\prec\cdots\prec x_r\prec x_{r+1}\prec\cdots\prec x_n$ 按吴定理而得的一系列不可约升列，且 ϕ_j 是升列 PC_j 中第一成员， $j=1,\cdots,r$, 则有自然数 s,

使得 $(\prod_{1\leqslant j\leqslant r}\phi_j)^s$ 是 $I\cap F[x_1,\cdots,x_r]$ 中非零多项式.

证明　首先证明: $\phi_j\in F[x_1,\cdots,x_r]$, $j=1,\cdots,r$. 假若对于某个 $k\in\{1,\cdots,r\}$, $\phi_k\notin F[x_1,\cdots,x_r]$. 记 $PC_k=\{g_1,\cdots,g_m\}$, 其中 $g_1=\phi_k$, 且设 x_{j_i} 为 g_i 的主变量, $i=1,\cdots,m$. 此时必有 $r<j_1<\cdots<j_m$. 不失一般性, 可设 $x_{j_i}=x_{r+i}$, $i=1,\cdots,m$. 由不可约升列的定义, 我们有如下域扩张塔:

$$K_0=F(V),\ K_1=K_0[x_{r+1}]/(g_1),\ \cdots,\ K_m=K_{m-1}[x_{r+m}]/(g_m)$$

其中 $V=\{x_1,\cdots,x_r,x_{r+m+1},\cdots,x_n\}$, 且 (g_i) 为 $K_{i-1}[x_{r+i}]$ 中由 g_i 生成的理想, $i=1,\cdots,m$.

记 $\bar{x}_i$ 为 x_i 在从 $F[\overline{X}]$ 到 K_m 的典范同态下的象, $i=1,\cdots,n$. 显然, $(\bar{x}_1,\cdots,\bar{x}_n)\in\text{Zero}(PC_k/I_k)\subseteq\text{Zero}(PS)$. 因而, $(\bar{x}_1,\cdots,\bar{x}_n)$ 也是 I 的一个零点. 由所设, 在 $I\cap F[x_1,\cdots,x_r]$ 中有一个非零多项式 h. 于是有

$$h(\bar{x}_1,\cdots,\bar{x}_r)=h(\bar{x}_1,\cdots,\bar{x}_n)=0.$$

然而, $\bar{x}_1,\cdots,\bar{x}_r$ 在 F 上显然是代数无关的, 矛盾. 因而, $\phi_j\in F[x_1,\cdots,x_r]$, $j=1,\cdots,r$.

由上面的吴定理, 我们有 $\prod_{1\leqslant j\leqslant r}\phi_j(\alpha)=0$, 只要 $\alpha\in\text{Zero}(PS)$. 再根据熟知的 Hilbert 零点定理, 证明将可完成.

由上面诸引理, 我们可以建立下面的定理.

定理 9.2.6　设记号同上, 则可有效地计算出一个单元多项式 $p(x_n)$, 使得对于 $\mathcal{S}_R(f,x_n)$ 的每个有限开端点 a, $p(a)=0$.

证明　根据上面引理, 我们可以执行如下有效计算.

(1) 借助于吴方法, 我们可获得 $\{f+t,\dfrac{\partial f}{\partial x_i},i=1,\cdots,n-1\}$ 关于序 $t\prec x_n\prec\{x_1,\cdots,x_{n-1}\}$ 的一系列不可约升列 $PC_1,\cdots,PC_r$. 记 ϕ_i 为 PC_i 中的第一成员, 且令 $\phi=\prod_{1\leqslant i\leqslant r}\phi_i$. 由引理 9.2.2 和 9.2.5 知, 对于某个 $s\in\mathbb{N}$, ϕ^s 是 $I\cap F[t,x_n]$ 中非零多项式. 记 $e(x_n)$ 为 ϕ 作为 $F[x_n]$ 上含单变量 t 的多项式的尾项系数. 显然 $e(x_n)\in F[x_n]$.

(2) 对于每个整数组 $(j_1,\cdots,j_k)$, 其中 $1\leqslant j_1<\cdots<j_k\leqslant n-1$, 由引理 9.2.2 有 $I\cap F[t,x_{j_1},\cdots,x_{j_k},x_n]\neq\{0\}$, 这里 I 是 $F[t,\overline{X}]$ 中由 $\{f+t,\dfrac{\partial f}{\partial x_i},i\in\{1,2,\cdots,n-1\}\backslash\{j_1,\cdots,j_k\}\}$ 生成的理想. 借助于吴方法, 我们可获得 $\{f+t,\dfrac{\partial f}{\partial x_i},i\in\{1,2,\cdots,n-1\}\backslash\{j_1,\cdots,j_k\}\}$ 关于序 $t\prec x_n\prec\{x_{j_1},\cdots,x_{j_k}\}\prec\{x_1,\cdots,x_{n-1}\}\backslash\{x_{j_1},\cdots,x_{j_k}\}$ 的一系列不可约升列 $PC_1,\cdots,PC_r$. 在 PC_i 中取出第一成员 ψ_i,

$i=1,\cdots,r$, 且令 $\psi_{j_1\cdots j_k}=\prod\limits_{1\leqslant i\leqslant r}\psi_i$. 由引理 9.2.5 知, 对于某个 $s_{j_1\cdots j_k}\in\mathbb{N}$, $\psi_{j_1\cdots j_k}^{s_{j_1\cdots j_k}}$ 是 $I\cap F[t,x_{j_1},\cdots,x_{j_k},x_n]$ 中非零多项式.

(3) 对于在过程 (2) 中所得的每个多项式 $\psi_{j_1\cdots j_k}$, 记 $u_{j_1\cdots j_k}(x_n,t)$ 为 $\psi_{j_1\cdots j_k}$ 作为 $F(x_n,t)$ 上多项式关于字典序: $x_{j_1}\prec\cdots\prec x_{j_k}$ 的首项系数. 又记 $e_{j_1\cdots j_k}(x_n)$ 为 $u_{j_1\cdots j_k}(x_n,t)$ 作为 $F[x_n]$ 上含单变量 t 的多项式的尾项系数. 显然, $e_{j_1\cdots j_k}(x_n)\in F[x_n]$.

令 $p(x_n):=e(x_n)\prod\limits_{\lambda}e_\lambda(x_n)$, 其中指标 λ 取遍所有满足 $1\leqslant j_1<\cdots<j_k\leqslant n-1$ 的整数组 $(j_1,\cdots,j_k)$. 此时, 可以断定多项式 $p(x_n)$ 正为所求. 事实上, $e_{12\cdots(n-1)}(x_n)$ 显然是 f 作为 $F(x_n)$ 上多项式关于字典序 $x_1\prec\cdots\prec x_{n-1}$ 的首项系数. 对于 $\mathcal{S}_R(f,x_n)$ 的每个有限端点 a, 由引理 9.2.3 知, $e_{12\cdots(n-1)}(a)=0$, 或者 $\mathcal{V}_{R_{\langle 0\rangle}}(f_+,x_n)$ 有一个有限端点 a^*, 使得 a^*-a 在 R 上是无限小. 当 $e_{12\cdots(n-1)}(a)=0$ 时, 显然 $p(a)=0$. 现假定对于 $\mathcal{V}_{R_{\langle 0\rangle}}(f_+,x_n)$ 的某个有限端点 a^*, a^*-a 在 R 上是无限小.

当 a^* 是 $\mathcal{V}_{R_{\langle 0\rangle}}(f_+,x_n)$ 的一个闭端点时, 由引理 9.2.2 知, $\phi^s(\epsilon_0,a^*)=0$, 即 $\phi(\epsilon_0,a^*)=0$. 设 t^s $(s\geqslant 0)$ 是 $\phi(t,x_n)$ 作为 $F[x_n]$ 上含单变量 t 的多项式的尾项, 则 $\phi(t,x_n)=t^s\phi_0(t,x_n)$, 这里 $\phi_0(t,x_n)\in F[t,x_n]$. 于是 $\epsilon_0^s\phi_0(\epsilon_0,a^*)=0$, 即 $\phi_0(\epsilon_0,a^*)=0$. 从而 $e(a)=\phi_0(0,a)=\phi_0(\pi(\epsilon_0),\pi(a^*))=\pi(\phi_0(\epsilon_0,a^*))=0$. 现考虑这种情况: a^* 是 $\mathcal{V}_{R_{\langle 0\rangle}}(f_+,x_n)$ 的一个开端点. 由引理 9.2.4 知, 对于某个整数组 $(j_1,\cdots,j_k)$, 其中 $1\leqslant j_1<\cdots<j_k\leqslant n-1$, 以及某些 $\varrho_1,\cdots,\varrho_k\in\{1,-1\}$, $\mathcal{V}_{R_{\langle k\rangle}}(h,x_n)$ 有一个闭端点 a_n^*, 使得 $\pi_0(a_n^*)=a^*$, 这里 h 是在 f_+ 中通过代换: $x_{j_i}=\varrho_i\epsilon_i^{-1}$, $i=1,\cdots,k$, 而得到的 $F_{\langle k\rangle}$ 上多项式. 由引理 9.2.2 有, $\psi_{j_1\cdots j_k}^{s_{j_1\cdots j_k}}(\epsilon_0,\varrho_1\epsilon_1^{-1},\cdots,\varrho_k\epsilon_k^{-1},a_n^*)=0$, 即 $\psi_{j_1\cdots j_k}(\epsilon_0,\varrho_1\epsilon_1^{-1},\cdots,\varrho_k\epsilon_k^{-1},a_n^*)=0$. 假若 $u_{j_1\cdots j_k}(\epsilon_0,a_n^*)$ 在 $R_{\langle 0\rangle}$ 上不是无限小, 则对于某个正元素 $d\in R_{\langle 0\rangle}$, $u_{j_1\cdots j_k}(\epsilon_0,a_n^*)^2>d$. 显然, 多项式 $\psi_{j_1\cdots j_k}(t,\varrho_1x_{j_1},\cdots,\varrho_kx_{j_k},x_n)$ 可表为

$$\begin{aligned}&\psi_{j_1\cdots j_k}(t,\varrho_1x_{j_1},\cdots,\varrho_kx_{j_k},x_n)\\=\;&\pm u_{j_1\cdots j_k}(t,x_n)x_{j_1}^{r_1}\cdots x_{j_k}^{r_k}+\sum_{i_1\cdots i_k}w_{i_1\cdots i_k}(t,x_n)x_{j_1}^{i_1}\cdots x_{j_k}^{i_k},\end{aligned}$$

其中 $u_{j_1\cdots j_k}(t,x_n)x_{j_1}^{r_1}\cdots x_{j_k}^{r_k}$ 是 $\psi_{j_1\cdots j_k}$ 作为 $F(x_n,t)$ 上多项式关于字典序 $x_{j_1}\prec\cdots\prec x_{j_k}$ 的首项系数, 且 $w_{i_1\cdots i_k}(t,x_n)\in F[t,x_n]$.

由等式 $\psi_{j_1\cdots j_k}(\epsilon_0,\varrho_1\epsilon_1^{-1},\cdots,\varrho_k\epsilon_k^{-1},a_n^*)=0$, 我们有

$$\begin{aligned}d<\;&u_{j_1\cdots j_k}(\epsilon_0,a_n^*)^2\\=\;&\pm u_{j_1\cdots j_k}(\epsilon_0,a_n^*)\sum_{i_1\cdots i_k}w_{i_1\cdots i_k}(\epsilon_0,a_n^*)\epsilon_1^{r_1-i_1}\cdots\epsilon_k^{r_k-i_k}.\end{aligned}$$

对于每个对应于较低项 $x_{j_1}^{i_1}\cdots x_{j_k}^{i_k}$ 的数组 $(i_1,\cdots,i_k)$, 如下元素在 $R_{\langle 0\rangle}$ 上是无

限小:

$$u_{j_1\cdots j_k}(\epsilon_0,a_n^*)w_{i_1\cdots i_k}(\epsilon_0,a_n^*)\epsilon_1^{r_1-i_1}\cdots\epsilon_k^{r_k-i_k}.$$

从而, 上面的不等式不可能成立. 这表明 $u_{j_1\cdots j_k}(\epsilon_0,a_n^*)$ 在 $R_{\langle 0\rangle}$ 上是无限小. 因而, $\pi_0\Big(u_{j_1\cdots j_k}(\epsilon_0,a_n^*)\Big)=0$, 即 $u_{j_1\cdots j_k}(\epsilon_0,a^*)=0$. 设 t^s $(s\geqslant 0)$ 是 $u_{j_1\cdots j_k}(t,x_n)$ 作为 $F[x_n]$ 上含单变量 t 的多项式的尾项, 则 $u_{j_1\cdots j_k}(t,x_n)=t^s v(t,x_n)$, 其中 $v(t,x_n)\in F[t,x_n]$. 于是有 $\epsilon_0^s v(\epsilon_0,a^*)=0$, 即 $v(\epsilon_0,a^*)=0$. 因而 $e_{j_1\cdots j_k}(a)=v(0,a)=v\Big(\pi(\epsilon_0),\pi(a^*)\Big)=\pi\Big(v(\epsilon_0,a^*)\Big)=0$.

这样, 在任何情况下都有 $p(a)=0$. 证毕.

现在, 我们可建立下面的主要定理.

定理 9.2.7 设 $(F,\leqslant)$ 是一个实闭包为 R 的可计算序域, $f(\overline{X})$ 是 F 上一个 n 元多项式, 且 $n\geqslant 2$. 若 F 容纳一个有效方法, 使得每个非零单元多项式都能找到一个隔离集, 则可有效地计算出 F 的一个有限子集 $\varGamma$, 使得 $f(\overline{X})$ 是半正定的, 当且仅当对于每个 $a\in\varGamma$, $f(x_1,\cdots,x_{n-1},a)$ 是半正定的.

证明 由定理 9.2.6 知, 可有效地计算出一个单元多项式 $p(x_n)$, 使得对于 $\mathcal{S}_R(f,x_n)$ 的每个有限开端点 a, $p(a)=0$. 由所设, 我们可有效地求出 $p(x_n)$ 的一个隔离集 $\varGamma$.

很清楚, 若对于某个 $a\in\varGamma$, $f(x_1,\cdots,x_{n-1},a)$ 不是半正定的, 则 $f(\overline{X})$ 不是半正定的. 现设 $f(\overline{X})$ 不是半正定的, 则 $\mathcal{S}_R(f,x_n)\neq\varnothing$. 当 $\mathcal{S}_R(f,x_n)=R$ 时, 显然对于任意 $a\in\varGamma$, $f(x_1,\cdots,x_{n-1},a)$ 不是半正定的. 当 $\mathcal{S}_R(f,x_n)\neq R$ 时, 至少存在 $\mathcal{S}_R(f,x_n)$ 的一个有限端点 a. 当然, a 是 $p(x_n)$ 的零点. 从而有 $b,c\in\varGamma$, 其中 $b<c$, 使得开区间 $]b,c[$ 仅包含 $\mathcal{S}_R(f,x_n)$ 的这一个端点 a. 因而, $b\in\mathcal{S}_R(f,x_n)$ 或 $c\in\mathcal{S}_R(f,x_n)$. 这表明 $f(x_1,\cdots,x_{n-1},b)$ 或 $f(x_1,\cdots,x_{n-1},c)$ 不是半正定的. 证毕.

作为判定多项式的半定性的两个初始阶段, 我们考虑三元多项式与二元多项式这两种特殊情形.

设 $f(x,y,z)$ 是 F 上一个三元多项式, 其中变量 x 或 y 真正在 $f(x,y,z)$ 中出现. 令 $f_x=\dfrac{\partial f}{\partial x}$ 且 $f_y=\dfrac{\partial f}{\partial y}$. 由吴方法, 我们可得到 $\{f+t,f_x,f_y\}$ 关于序 $z\prec y\prec x$ 的一系列不可约升列 $PC_1,\cdots,PC_r$. 令 $\phi=\prod\limits_{1\leqslant j\leqslant r}\phi_j$, 这里, ϕ_j 是 PC_j 中第一成员, $j=1,\cdots,r$. 由引理 9.2.2 和 9.2.5 知, $\phi\in F[t,z]$. 记 $u(z)$ 为 ϕ 作为 $F[z]$ 上多项式的尾项系数. 此外, 用 $\mathrm{Res}(f+t,f_x;x)$ 记作 $f+t$ 和 f_x 关于 x 的结式, 而 $\mathrm{Res}(f+t,f_y;y)$ 记作 $f+t$ 和 f_y 关于 y 的结式. 注意到, $f+t$ 是 $F[t,x,y,z]$ 中不可约多项式. 易知, $\mathrm{Res}(f+t,f_x;x)$, $\mathrm{Res}(f+t,f_y;y)$ 分别为 $F[t,y,z]$, $F[t,x,z]$ 中的非零多项式. 用 $h_1(t,z)$ (或 $h_2(t,z)$) 表示 $\mathrm{Res}(f+t,f_x;x)$ (或 $\mathrm{Res}(f+t,f_y;y)$) 作为 $F[t,z]$ 上多项式的首项系数, 并记 $v(z)$ 为 $h_1(t,z)h_2(t,z)$ 作为 $F[z]$ 上多项式

的尾项系数.

定理 9.2.8 设记号同上, 且 $e(z)$ 是 $f(x,y,z)$ 作为 $F[z]$ 上多项式关于序: $x \prec y$ 的首项系数. 如果 Γ 是 $u(z)v(z)e(z)$ 的一个隔离集, 则 $f(x,y,z)$ 是半正定的, 当且仅当对于每个 $a \in \Gamma$, $f(x,y,a)$ 是半正定的.

证明 设 J_1 和 J_2 分别是 $F[t,k,x,y,z]$ 中由 $\{f+t, f_x\}$ 和 $\{f+t, f_y\}$ 生成的理想. 由关于多项式的结式的一个熟知事实 (见 [137] 中引理 7.2.1), $\mathrm{Res}(f+t, f_x; x) \in J_1 \cap F[t,z,y]$, 而 $\mathrm{Res}(f+t, f_y; y) \in J_2 \cap F[t,z,x]$. 根据定理 9.2.6 和 9.2.7 以及它们的证明, $u(z)v(z)e(z)$ 正是定理 9.2.7 中所要求的单元多项式. 因而, 定理成立.

现考虑二元多项式的半定性的判定. 设 $f(x,y) \in F[x,y]$ 是一个多项式, 其中变量 x 真正出现. 令 $f_x = \dfrac{\partial f(x,y)}{\partial x}$, 且用 $\mathrm{Res}(f+t, f_x; x)$ 表示 $f+t$ 和 f_x 关于 x 的结式. 同样, $\mathrm{Res}(f+t, f_x; x) \neq 0$. 记 $v(y)$ 为 $\mathrm{Res}(f+t, f_x; x)$ 作为 $F[y]$ 上含单变量 t 的多项式的尾项系数.

定理 9.2.9 设 $f(x,y)$, f_x 和 $v(y)$ 同上. 如果 Γ 是多项式 $v(y)$ 的一个隔离集, 则 $f(x,y)$ 在 R 上是半正定的, 当且仅当对于每个 $a \in \Gamma$, $f(x,a)$ 在 R 上是半正定的.

证明 记 I 为 $F[t,x,y]$ 中由 $f+t$ 和 f_x 生成的理想, 则 $\mathrm{Res}(f+t, f_x; x) \in I \cap F[t,y]$. 用 $e(y)$ 表示 f 作为 $F[y]$ 上多项式的首项系数. 很清楚, $e(y)$ 也是 $f+t$ 作为 $F[t,y]$ 上多项式的首项系数. 由定理 9.2.6 及其证明知, $e(y)v(y)$ 恰是定理 9.2.6 中所要求的单元多项式. 注意到, 若把 $e(y)$ 的任意一个零点代入 $\mathrm{Res}(f+t, f_x; x)$ 中的变量 y, 则 $\mathrm{Res}(f+t, f_x; x)$ 都将变为零. 从而, $e(y)$ 的每个零点也是 $v(y)$ 的零点. 于是, Γ 也是 $e(y)v(y)$ 的一个隔离集.

由定理 9.2.7 及其证明知, $f(x,y)$ 在 R 上是半正定的, 当且仅当对于每个 $a \in \Gamma$, $f(x,a)$ 在 R 上是半正定的. 证毕.

鉴于定理 9.2.6 和 9.2.7, 我们有一个算法, 使得在多项式的半正定性的判定中, 可将所给多项式简化为一些含较少变量的多项式. 对于一个真正含有变量 x_n 的输入多项式 $f \in F[x_1, \cdots, x_n]$, 我们的算法由如下步骤组成:

(1) 借助于吴方法, 我们可获得 $\{f+t, \dfrac{\partial f}{\partial x_i}, i=1, \cdots, n-1\}$ 关于序 $t \prec x_n \prec \{x_1, \cdots, x_{n-1}\}$ 的一系列不可约升列 $PC_1, \cdots, PC_r$. 记 ϕ_i 为 PC_i 中的第一成员, 且令 $\phi = \prod\limits_{1 \leqslant i \leqslant r} \phi_i$. 由引理 9.2.2 和 9.2.5 知, ϕ 是 $I \cap F[t, x_n]$ 中非零多项式. 记 $e(x_n)$ 为 ϕ 作为 $F[x_n]$ 上含单变量 t 的多项式的尾项系数.

(2) 对于每个整数组 $(j_1, \cdots, j_k)$, 其中 $1 \leqslant j_1 < \cdots < j_k \leqslant n-1$, 由引理 9.2.2 有 $I \cap F[t, x_{j_1}, \cdots, x_{j_k}, x_n] \neq \{0\}$, 这里 I 是 $F[t, \overline{X}]$ 中由 $\{f+t, \dfrac{\partial f}{\partial x_i}, i \in \{1,2,\cdots,n-1\} \setminus \{j_1, \cdots, j_k\}\}$ 生成的理想. 借助于吴方法, 我们可获得 $\{f+t, \dfrac{\partial f}{\partial x_i},$

$i \in \{1, 2, \cdots, n-1\} \backslash \{j_1, \cdots, j_k\}\}$ 关于序 $t \prec x_n \prec \{x_{j_1}, \cdots, x_{j_k}\} \prec \{x_1, \cdots, x_{n-1}\} \backslash \{x_{j_1}, \cdots, x_{j_k}\}$ 的一系列不可约升列 $PC_1, \cdots, PC_r$. 在 PC_i 中取出第一成员 ψ_i, $i = 1, \cdots, r$, 且令 $\psi_{j_1 \cdots j_k} = \prod_{1 \leqslant i \leqslant r} \psi_i$.

(3) 对于在过程 (2) 中所得的每个多项式 $\psi_{j_1 \cdots j_k}$, 记 $u_{j_1 \cdots j_k}(x_n, t)$ 为 $\psi_{j_1 \cdots j_k}$ 作为 $F(x_n, t)$ 上多项式关于字典序 $x_{j_1} \prec \cdots \prec x_{j_k}$ 的首项系数. 又记 $e_{j_1 \cdots j_k}(x_n)$ 为 $u_{j_1 \cdots j_k}(x_n, t)$ 作为 $F[x_n]$ 上含单变量 t 的多项式的尾项系数.

(4) 确定 $e(x_n) \prod_{\lambda} e_\lambda(x_n)$ 的一个隔离集 Γ, 其中 λ 取遍所有满足 $1 \leqslant j_1 < \cdots < j_k \leqslant n-1$ 的整数组 $(j_1, \cdots, j_k)$.

作为上面过程的输出, 获得由 $n-1$ 元多项式组成的集合 $\{f(x_1, \cdots, x_{n-1}, a) \mid a \in \Gamma\}$, 使得 f 是半正定 (或半负定) 当且仅当 $\{f(x_1, \cdots, x_{n-1}, a) \mid a \in \Gamma\}$ 中每个成员是半正定 (或半负定).

例 判定多项式 $f(x, y)$ 是否是半正定的, 这里 $f(x, y) = 2x^6 - 3x^4y^2 + y^6 + x^2y^2 - 6y + 5$.

解 根据定理 9.2.9, 我们进行如下计算.

(1) 计算 $f + t$ 和 $\dfrac{\partial f}{\partial x}$ 关于 x 的结式如下:

$$
\begin{aligned}
& \mathrm{Res}(f + t, \frac{\partial f}{\partial x}; x) \\
= \ & (y^6 - 6y + 5 + t)(43200 + 8768y^6 + 8640y^4 - 103680y + 1728y^{10} \\
& -144y^8 - 10368y^5 + 1728y^4t - 10368y^7 + 62208y^2 - 20736yt \\
& +1728y^6t + 1728t^2)^2.
\end{aligned}
$$

(2) 作为 $\mathbb{Q}[y]$ 上含单变量 t 的一个多项式, $\mathrm{Res}(f + t, \frac{\partial f}{\partial x}; x)$ 的尾项系数为

$$
\begin{aligned}
v(y) := \ & (y^6 - 6y + 5)(43200 + 8768y^6 + 8640y^4 - 103680y \\
& +1728y^{10} - 144y^8 - 10368y^5 - 10368y^7 + 62208y^2)^2.
\end{aligned}
$$

(3) 求出 $v(y)$ 的一个如下隔离集 Γ:

$$
\Gamma = \{\frac{15}{16}, \frac{31}{32}, \frac{21}{16}, \frac{43}{32}\}.
$$

(4) 对于每个 $a \in \Gamma$, 判定单元多项式 $f(x, a)$ 是否是半正定的. 由计算, 我们有

$$
f(x, \frac{31}{32}) = 2x^6 - \frac{2883}{1024}x^4 + \frac{961}{1024}x^2 + \frac{15088449}{1073741824}.
$$

容易判别, $f(x, \frac{31}{32})$ 有一个实的单根. 这意味着 $f(x, \frac{31}{32})$ 不是半正定的. 因而, $f(x, y)$ 不是半正定的.

借助于计算机代数系统 Maple V Release 4, 上面算法被编制成一个适用于有理系数多项式的通用程序. 在一台内存为 128 MB 的 PentiumIV 计算机上, 下列实例被处理.

实例 (1)$x^4+2x^2z+x^2-2xyz+2y^2z^2-2yz^2+2z^2-2x+2yz+1/2$;

(2)$x^4+2x^2z+x^2-2xyz+2y^2z^2-2yz^2+2z^2-2x+2yz+1$;

(3)$x^4y^4-2x^5y^3z^2+x^6y^2z^4+2x^2y^3z-4x^3y^2z^3+2x^4yz^5+z^2y^2-2z^4yx+z^6x^2$;

(4)$x^4y^4-2x^5y^3z^2+x^6y^2z^4+2x^2y^3z-4x^3y^2z^3+2x^4yz^5+z^2y^2-2z^4yx+99/100z^6x^2$.

对每小题的回答分别是: "$\left[\frac{1}{2},-\frac{7}{2},\frac{1}{16}\right]$", "true", "true" 和 "$[-1,1-1]$", 其中词 "true" 表示对应的多项式是半正定的, 而数组 "$[a,b,c]$" 表示当 $[x,y,z]=[a,b,c]$ 时, 对应的多项式的值为负. 各自的 CPU 时间为: 0.4 秒, 0.2 秒, 0.3 秒和 18.5 秒.

§9.3 代数方程组有实解的非标准判定

对于系数在域 F 中的多项式方程组, 通过著名的吴方法以及 Gröbner 基方法都可有效地判定该方程组在 F 的代数闭包中是否有解. 然而当系数域 F 是一个序域, 且要判定该方程组是否在 F 的实闭包中是否有解时, 问题要更为复杂. 在 §9.1 中, 我们给出了判定实多项式方程是否有实解的两个判别定理, 并在此基础上研究了二元多项式的实零点的存在性. 本节的目的是给出一个有效算法, 用来判定一个 n 元多项式方程组是否在系数域的实闭包中有实解. 作为一个并存的结果, 我们同时获得了判定多元多项式是否半定的另一有效方法.

和 §9.1 的方法一样, 本节的方法也是非标准的. 用 $(F,\leqslant)$ 表示实闭包为 R 的一个可计算的序域, $F_{\langle n\rangle}$ 表示在 F 上添加无限小正元素 $t_1=t, t_2, \cdots, t_n$ 所得到的非阿基米德序域, 其实闭包记作 $R_{\langle n\rangle}$. 用 $F[\overline{X}]:=F[x_1,\cdots,x_n]$ 表示域 F 上的 n 元多项式环, 这里 $n\geqslant 2$. 此外, 对于 $F_{\langle s\rangle}[\overline{X}]$ 的一个有限子集 E, 其中 $1\leqslant s\leqslant n$, 若 E 所涉及的未定元集为 $U(\subseteq\overline{X})$, 则用 $\dim(E)$ 表示 $F_{\langle s\rangle}[U]$ 中由 E 生成的理想的 Krull 维数, 并直接称 $\dim(E)$ 为 E 的维数或方程组 $f=0, f\in E$ 的维数.

首先, 我们需要建立有关引理. 对于域 L 的一个扩张 Ω, 用 $\mathrm{tr.deg}(\Omega/L)$ 表示 Ω 在 L 上的超越次数.

引理 9.3.1 设 Ω 是域 L 是任意一个域扩张, $f\in L[x_1,\cdots,x_n]$, 且 f 是在环 $L[x_1,\cdots,x_{n-1}]$ 上含 x_n 的本原多项式. 若有 $\xi_1,\cdots,\xi_n\in\Omega$, 使得 $f(\xi_1,\cdots,\xi_n)=0$, 且 $\mathrm{tr.deg}(L(\xi_1,\cdots,\xi_n)/L)=n-1$, 则 $\xi_1,\cdots,\xi_{n-1}$ 在 L 上代数无关.

证明 假若 $\xi_1,\cdots,\xi_{n-1}$ 在 L 上代数相关, 则 ξ_n 必是域 $L(\xi_1,\cdots,\xi_{n-1})$ 上的超越元素. 令 $f=g_dx_n^d+g_{d-1}x_n^{d-1}+\cdots+g_0$, 其中 $g_i\in L[x_1,\cdots,x_{n-1}]$, $i=0,1,\cdots,d$.

则由 $f(\xi_1,\cdots,\xi_n)=0$ 可推出 $g_i(\xi_1,\cdots,\xi_{n-1})=0, i=0, 1, \cdots, d$. 不失一般性，设 ξ_1 是域 $L(\xi_2,\cdots\xi_{n-1})$ 上的代数元. 这表明诸单元多项式 $g_i(x_1,\xi_2,\cdots,\xi_{n-1}), i=0, 1, \cdots, d$, 具有非常量公因式. 注意到 $x_1, \xi_2, \cdots, \xi_{n-1}$ 在 L 上代数无关，从而诸多项式 $g_0, g_1, \cdots, g_d$ 也具有非常量公因式，这矛盾于 f 的本原性. 证毕.

引理 9.3.2 设 $f\in F[\overline{X}]$, 且 f 是在 $F[x_1,\cdots,x_{n-1}]$ 上含 x_n 的本原多项式. 若 f 在 R 中不是半定的，则有 $\xi_1, \cdots, \xi_n\in R_{\langle n\rangle}$, 使得 $f(\xi_1,\cdots,\xi_n)=0$, 且 $\xi_1, \cdots, \xi_{n-1}$ 在 F 上代数无关.

证明 由于 f 在 R 中不是半定的，从而，对于某两个 $\alpha=(a_1,\cdots,a_n)$, $\beta=(b_1,\cdots,b_n)\in R^n$, $f(\alpha)f(\beta)<0$. 令 $\beta^*=(b_1+t_1,\cdots,b_n+t_n)\in R^n_{\langle n\rangle}$. 注意到 $f(\alpha)f(\beta^*)$ 是 $R_{\langle n\rangle}$ 上含 $t_1, \cdots, t_n$ 的多项式，且其常数项为 $f(\alpha)f(\beta)<0$. 由 $R_{\langle n\rangle}$ 的序结构，我们有 $f(\alpha)f(\beta^*)<0$. 作 $R_{\langle n\rangle}$ 上单元多项式 $\Psi(y):=f(a_1(1-y)+(b_1+t_1)y,\cdots,a_n(1-y)+(b_n+t_n)y)$, 则 $\Psi(0)\Psi(1)=f(\alpha)f(\beta^*)<0$. 由多项式的中间值定理，有 $\lambda\in R_{\langle n\rangle}$, 使得 $\Psi(\lambda)=0$, 且 $0<\lambda<1$. 记 $\xi_i=a_i(1-\lambda)+(b_i+t_i)\lambda$, $i=1, \cdots, n$, 则 $t_i=(\xi_i-a_i+a_i\lambda)/\lambda-b_i\in R(\xi_1,\cdots,\xi_n,\lambda)$, $i=1, \cdots, n$. 由于 $t_1, \cdots, t_n$ 在 R 上是代数无关的，从而 $\mathrm{tr.deg}(R(\xi_1,\cdots,\xi_n,\lambda)/R)\geqslant n$. 于是, $\mathrm{tr.deg}(R(\xi_1,\cdots,\xi_n)/R)\geqslant n-1$. 另一方面，显然 $\mathrm{tr.deg}(R(\xi_1,\cdots,\xi_n)/R)\leqslant n$, 因为 $(\xi_1,\cdots,\xi_n)$ 是非零多项式 f 的一个零点. 从而 $\mathrm{tr.deg}(R(\xi_1,\cdots,\xi_n)/R)=n-1$. 再由引理 9.3.1 知， $\xi_1, \cdots, \xi_{n-1}$ 在 R 上是代数无关的. 证毕.

借助于 Gröbner 基的有关理论，我们可证明了本节中如下主要结果.

定理 9.3.3 设 I 是由 $F[\overline{X}]$ 中多项式 $f_1, \cdots, f_r$ 生成的理想， $\{x_1, \cdots, x_m\}$ 是一个模于 I 的极大无关变元组，I^e 是 I 在 $F(x_1,\cdots,x_m)[x_{m+1},\cdots,x_n]$ 上的扩理想，且 I^e 关于变元 x_{m+1} 处于正规位置. 若 G 是 I 关于字典序 $x_1\prec\cdots\prec x_m\prec x_{m+1}\prec\cdots\prec x_n$ 的简化 Gröbner 基，则对于 G 中首项最低的元素 g_0, 有 $g_0=uh$, 这里 $u\in F[x_1,\cdots,x_m]$, h 是 $F[x_1,\cdots,x_m]$ 上一个含 x_{m+1} 的本原多项式，且方程组 $f_i=0, i=1, \cdots, r$, 在 R 中有解当且仅当下列三个条件之一成立:

(1) 方程组

$$\begin{cases} u=0, \\ f_i=0, \quad i=1,\cdots,r \end{cases}$$

在 R 中有解;

(2) 多项式 h 在 R 中不是半定的;

(3) 方程组

$$\begin{cases} f_i &=0, i=1,\cdots,r \\ \dfrac{\partial h}{\partial x_j} &=0, j=1,\cdots,m+1 \end{cases}$$

在 R 中有解.

证明 由所设, 我们有 $G \cap F[x_1, \cdots, x_m, x_{m+1}] \neq \varnothing$, 因为 $\{x_1, \cdots, x_m\}$ 是一个模于 I 的极大无关变元组. 由于 g_0 是 G 中首项最低的多项式, 从而 $g_0 \in F[x_1, \cdots, x_m, x_{m+1}]$, 其中未定元 x_{m+1} 真正出现在 g_0 中. 因而, g_0 可以写作 $g = uh$, 这里 $u \in F[x_1, \cdots, x_m]$, h 是 $F[x_1, \cdots, x_m]$ 上一个含 x_{m+1} 的本原多项式.

下面证明: 方程组 $f_i = 0$, $i = 1, \cdots, r$, 在 R 中有解当且仅当条件 (1), (2) 和 (3) 中之一成立.

必要性. 设方程组 $f_i = 0$, $i = 1, \cdots, r$, 在 R 中有解 $\overline{X} = \alpha = (a_1, \cdots, a_n)$. 由于 $g_0 \in I$, 从而 $g_0(\alpha) = 0$, 即 $u(\alpha)h(\alpha) = 0$. 当 $u(\alpha) = 0$ 时, 条件 (1) 成立. 现设 $h(\alpha) = 0$. 如若条件 (2) 不成立, 即 h 在 R 中是半定的. 于是, 单元多项式 $h_k = h(a_1, \cdots, a_{k-1}, x_k, a_{k+1}, \cdots, a_{m+1})$ 在 R 中也是半定的, $k = 1, \cdots, m+1$. 这表明 $x_k = a_k$ 是 h_k 的重根, 从而也是微商 h_k' 的根. 由此有, $\dfrac{\partial h}{\partial x_k}(\alpha) = h_k'(a_k) = 0$. 从而条件 (3) 成立. 必要性获证.

充分性. 由于 I^e 关于 x_{m+1} 处于正规位置, 从而由文献 [22] 中命题 8.77 知, I^e 关于字典序 $x_{m+1} \prec \cdots \prec x_n$ 的简化 Gröbner 基具有如下形式:

$$G^e = \{h_{m+1}, x_{m+2} - h_{m+2}, \cdots, x_n - h_n\}$$

这里 $h_i \in F(x_1, \cdots, x_m)[x_{m+1}]$, $i = m+1, \cdots, n$.

将 h_{m+1} 表示为 $h_{m+1} = vh^*$, 其中 $v \in F(x_1, \cdots, x_m)$, h^* 是 $F[x_1, \cdots, x_m]$ 上一个含 x_{m+1} 的本原多项式. 注意到, $g_0 \in I \cap F[x_1, \cdots, x_m, x_{m+1}] \subseteq I^e \cap F(x_1, \cdots, x_m)[x_{m+1}]$, 且 $I^e \cap F(x_1, \cdots, x_m)[x_{m+1}]$ 是由 h_{m+1} 生成的主理想. 从而在环 $F(x_1, \cdots, x_m)[x_{m+1}]$ 中, h_{m+1} 整除 g_0, 自然 h^* 整除 h. 由于 h^* 在 $F[x_1, \cdots, x_m]$ 上是本原的, 从而由 Gauss 引理的一个熟知推论 (见文献 [200] 第 33 页中引理 2) 知, 在 $F[x_1, \cdots, x_m, x_{m+1}]$ 中, h^* 整除 h. 另一方面, 由 I^e 的结构知, 有非零 $w \in F[x_1, \cdots, x_m]$, 使得 $wh^* \in I$. 从而 wh^* 可由 Gröbner 基 G 简化成零. 假若 h^* 是 h 的真因式, 则易知, 关于字典序 $x_1 \prec \cdots \prec x_m \prec x_{m+1} \prec \cdots \prec x_n$, wh^* 的首项低于 g_0 的首项, 从而低于 G 中每个元素的首项. 这样, 由文献 [22] 中定义 5.18 知, wh^* 是模于 G 的规范形, 矛盾. 因而, h 整除 h^*, 即 h^* 和 h 相伴. 不失一般性, 不妨设 $h^* = h$.

显然, 条件 (1) 或 (3) 都蕴含结论方程组 $f_i = 0$, $i = 1, \cdots, r$, 在 R 中有解. 当条件 (2) 成立时, 由引理 9.3.2 知, 有 $\xi_1, \cdots, \xi_{m+1} \in R_{<n>}$, 使得 $h(\xi_1, \cdots, \xi_{m+1}) = 0$, 且 $\xi_1, \cdots, \xi_m$ 在 F 上代数无关. 于是有从域 $F(x_1, \cdots, x_m)$ 到域 $F(\xi_1, \cdots, \xi_m)$ 的一个 F- 同构 τ, 使得 $\tau(x_i) = \xi_i$, $i = 1, \cdots, m$. 令 $\xi_j = h_j(\xi_1, \cdots, \xi_{m+1})$, $j = m+2. \cdots, n$, 则 τ 可拓展成 $F(x_1, \cdots, x_m)[x_{m+1}, \cdots, x_n]$ 到 $F(\xi_1, \cdots, \xi_m)[\xi_{m+1}, \cdots, \xi_n]$ 的一个同态 σ, 使得 $\sigma(x_j) = \xi_j$, $j = m+1, \cdots, n$. 对于每个 $i \in \{1, \cdots, n\}$, $f_i \in I \subseteq I^e$,

从而 f_i 可表示为

$$f_i = e_{m+1}h_{m+1} + e_{m+2}(x_{m+2} - h_{m+2}) + \cdots + e_n(x_n - h_n),$$

这里 $e_i \in F(x_1, \cdots, x_m)[x_{m+1}, \cdots, x_n]$, $i = m+1, \cdots, n$.

由此易知 $\sigma(f_i) = 0$, 即 $f_i(\xi_1, \cdots, \xi_n) = 0$, $i = 1, \cdots, r$. 再由适合实闭域的转移定理知, 方程组 $f_i(x_1, \cdots, x_n) = 0$, $i = 1, \cdots, r$, 在 R 中有解. 证毕.

当 $m = 0$, 即 I 是零维理想时, 我们立即得到下面的推论.

推论 设 I 是由 $F[\overline{X}]$ 中多项式 $f_1, \cdots, f_r$ 生成的零维理想, 且 I 关于未定元 x_1 处于正规位置, 则方程组 $f_i = 0$, $i = 1, \cdots, r$, 在 R 中有解, 当且仅当 h 在 R 中有实根, 这里 h 是 I 关于字典序 $x_1 \prec x_2 \prec \cdots \prec x_n$ 的简化 Gröbner 基中惟一含 x_1 的单元多项式.

由定理 9.3.3 可见, 方程组有实解的判定可简化到维数较低的情况以及元数较少的多项式的半定性的判定. 再结合下面的定理 9.3.4, 多项式的半定性的判定可进一步简化. 这样, 问题将最后归结到判定维数 $\leqslant 0$ 的方程组的实可解性以及单元多项式是否有实根.

鉴于定理 9.3.3, 要判定多项式方程组是否有实解, 需要一个判定多元多项式的半定性的有效方法. 对此, 我们将应用 §9.1 中定理 9.1.3 和引理 9.1.6 建立下面的定理, 这一定理可看作 §9.1 中定理 9.1.7 的一个推广.

定理 9.3.4 设 f 是 $F[\overline{X}]$ 中一个无重因式的多项式, 且 f 关于某一字典序的首项系数的符号为 $\epsilon(=\pm 1)$, 则 f 在 R 中是半定的, 当且仅当下面的叙述都成立:

(1) $f(x_1, \cdots, x_{n-1}, 0)$ 在 R 中是半定的;

(2) 对于每个 $i \in \{1, \cdots, n-1\}$, $f(x_1, \cdots, x_{i-1}, t^{-1}, x_{i+1}, \cdots, x_n)$ 在 $R_{\langle 1\rangle}$ 中是半定的;

(3) 对于每个 $i \in \{1, \cdots, n-1\}$, $f(x_1, \cdots, x_{i-1}, -t^{-1}, x_{i+1}, \cdots, x_n)$ 在 $R_{\langle 1\rangle}$ 中是半定的;

(4) 方程组

$$\begin{cases} f(\overline{X}) + \epsilon t &= 0 \\ \dfrac{\partial f}{\partial x_j} &= 0, \quad j = 1, \cdots, n-1 \end{cases}$$

在 $R_{\langle 1\rangle}$ 中无解.

证明 先证必要性. 设 f 在 R 中是半定的. 显然, 叙述 (1) 成立. 根据转移定理易知, 叙述 (2) 和 (3) 都成立. 此外, 由 §9.1 中引理 9.1.6 知, 叙述 (4) 也成立.

再证充分性. 设叙述 (1), (2), (3) 和 (4) 都成立. 为方便起见, 不妨设 $\epsilon = 1$. 令 $f_1 := f(\overline{X}) + t$. 设 f 关于字典序 $x_{i_1} \prec x_{i_2} \prec \cdots \prec x_{i_n}$ 的首项系数的符号为

1, 其中 $i_1, \cdots, i_n$ 是数字 1 到 n 的一个排列. 记 σ 是这样一个 n 级置换, 使得 $\sigma(i_k)=k$, $k=1,\cdots,n$. 注意到, $f(t_{\sigma(1)}^{-1},\cdots,t_{\sigma(n)}^{-1})$ 关于字典序 $t_1^{-1}\prec\cdots\prec t_n^{-1}$ 与 f 关于字典序 $x_{i_1}\prec\cdots\prec x_{i_n}$ 具有相同的首项系数. 由 $R_{\langle n\rangle}$ 的序结构知, $f(t_{\sigma(1)}^{-1},\cdots,t_{\sigma(n)}^{-1})>0$. 注意到, 对于 $i=1,\cdots,n$, 由对应 $t\mapsto t_i$ 所决定的从序域 $F(t)$ 到 $F(t_i)$ 的 F- 同构是保序的. 从而由叙述 (2) 知, 对于 $i=1,\cdots,n-1$, $g_i:=f(x_1,\cdots,x_{i-1},t_{\sigma(i)}^{-1},x_{i+1},\cdots,x_n)$ 在 $F(t_{\sigma(i)})$ 的实闭包中也是半定的. 由转移定理可知, g_i 在 $R_{\langle n\rangle}$ 中是半定的. 由于 $f(t_{\sigma(1)}^{-1},\cdots,t_{\sigma(n)}^{-1})>0$, 从而 g_i 在 $R_{\langle n\rangle}$ 中是半正定的. 又由于序域 $F(t_2)$ 和 $F(t_{\sigma(i)})$ 也是序同构的, 从而 $f(x_1,\cdots,x_{i-1},t_2^{-1},x_{i+1},\cdots,x_n)$ 在 $R_{\langle n\rangle}$ 中也是半正定的. 因此, 方程 $f(x_1,\cdots,x_{i-1},t_2^{-1},x_{i+1},\cdots,x_n)+t=0$ 即方程 $f_1(x_1,\cdots,x_{i-1},t_2^{-1},x_{i+1},\cdots,x_n)=0$ 在 $R_{\langle n\rangle}$ 中无解, $i=1,\cdots,n-1$.

此时, 我们可断定 $f(x_1,\cdots,x_{n-1},0)\neq 0$. 事实上, 如若不然, 则 $f=x_ng$, 这里 $g\in F[\overline{X}]$. 由上面讨论知, $f(t^{-1},\cdots,x_{n-1},x_n)$ 在 $R_{\langle n\rangle}$ 中是半正定的, 从而单元多项式 $f(t^{-1},\cdots,t_{n-1}^{-1},x_n)$ 在 $R_{\langle n\rangle}$ 中是半正定的. 这样, x_n 必是 $f(t^{-1},\cdots,t_{n-1}^{-1},x_n)$ 的偶因式. 由于 $t^{-1},\cdots,t_{n-1}^{-1}$ 在 F 上是代数无关的, 从而 x_n 也是 f 的偶因式, 与所设矛盾. 于是, 由叙述 (1) 知, $f(t^{-1},\cdots,t_{n-1}^{-1},0)>0$. 这表明 $f(x_1,\cdots,x_{n-1},0)$ 在 $R_{\langle n\rangle}$ 中是半正定的. 因此, 方程 $f(x_1,\cdots,x_{n-1},0)+t=0$ 即方程 $f_1(x_1,\cdots,x_{n-1},0)=0$ 在 $R_{\langle n\rangle}$ 中无解.

对于每个 $i\in\{1,\cdots,n-1\}$, 由叙述 (3) 和转移定理可知如下事实:

$$f(x_1,\cdots,x_{i-1},-t^{-1},x_{i+1},\cdots,x_n) \text{ 在 } R_{\langle n\rangle} \text{ 中是半定的.}$$

又由上面讨论知, 非零多项式 $f(x_1,\cdots,x_{n-1},0)$ 在 $R_{\langle n\rangle}$ 中是半正定的. 记 σ 是这样一个 $n-1$ 级置换, 使得 $\sigma(i)=1$. 由于 $-t_{\sigma(1)}^{-1},\cdots,-t_{\sigma(n-1)}^{-1}$ 在 F 上是代数无关的, 从而 $f(-t_{\sigma(1)}^{-1},\cdots,-t_{\sigma(i-1)}^{-1},-t^{-1},-t_{\sigma(i+1)}^{-1},\cdots,-t_{\sigma(n-1)}^{-1},0)>0$. 这表明 $f(x_1,\cdots,x_{i-1},-t^{-1},x_{i+1},\cdots,x_n)$ 在 $R_{\langle n\rangle}$ 中是半正定的. 由于序域 $F(t_2)$ 和 $F(t)$ 是序同构的, 从而可知如下事实:

$$f(x_1,\cdots,x_{i-1},-t_2^{-1},x_{i+1},\cdots,x_n) \text{ 在 } R_{\langle n\rangle} \text{ 中也是半正定的.}$$

因此, 对于每个 $i\in\{1,\cdots,n-1\}$, 方程 $f(x_1,\cdots,x_{i-1},-t_2^{-1},x_{i+1},\cdots,x_n)+t=0$ 即方程 $f_1(x_1,\cdots,x_{i-1},-t_2^{-1},x_{i+1},\cdots,x_n)=0$ 在 $R_{\langle n\rangle}$ 中无解.

再由叙述 (4) 知, 方程组 $f_1=0$, $\dfrac{\partial f_1}{\partial x_j}=0$, $j=1,\cdots,n-1$, 在 $R_{\langle 1\rangle}$ 无解. 注意到, t_2 是 $F_{\langle 1\rangle}$ 上的无限小正元素. 根据 §9.1 中定理 9.1.3, 方程 $f_1=0$ 在 $R_{\langle 1\rangle}$ 中无解. 最后由 §9.1 中引理 9.1.6 知, f 在 R 中是半定的. 证毕.

根据定理 9.1.4, 用同样的方法可建立下面的结论.

定理 9.3.5 设 $f\in F[\overline{X}]$, 且 f 关于某一字典序的首项系数的符号为 $\epsilon(=\pm1)$,

则 f 在 R 中是半定的，当且仅当下面的叙述都成立：

(1) 对于每个 $i \in \{1, \cdots, n\}$, $f(x_1, \cdots, x_{i-1}, t^{-1}, x_{i+1}, \cdots, x_n)$ 在 $R_{\langle 1 \rangle}$ 中是半定的；

(2) 对于每个 $i \in \{1, \cdots, n-1\}$, $f(x_1, \cdots, x_{i-1}, -t^{-1}, x_{i+1}, \cdots, x_n)$ 在 $R_{\langle 1 \rangle}$ 中是半定的；

(3) 方程组

$$\begin{cases} f(\overline{X}) + \epsilon t &= 0 \\ \dfrac{\partial f}{\partial x_j} &= 0, \quad j = 1, \cdots, n-1 \end{cases}$$

在 $R_{\langle 1 \rangle}$ 中无解.

定理 9.3.4 与定理 9.3.5 表明，无重因式的 n 元多项式的半定性的判定可简化成判定 $n-1$ 元多项式的半定性以及判定维数小于 n 的方程组是否有实解.

在定理 9.3.3 和 9.3.4(或 9.3.5) 的基础上，并借助于 Gröbner 基的有关算法，可给出判定多元多项式的半定性以及多项式方程组是否有实解的算法. 鉴于定理 9.3.3, 首先要考虑的问题是：对于 $F[\overline{X}]$ 的一个理想 I, 怎样求出一个模于 I 的极大无关变元组. 在下面，我们给出一个求极大无关变元组的简单算法.

引理 9.3.6 设 I 是 $F[\overline{X}]$ 的一个非零的真理想，且 G 是 I 关于字典序 $x_{j_1} \prec x_{j_2} \prec \cdots \prec x_{j_n}$ 的简化 Gröbner 基，则如下集合

$$W = \{x_{j_i} \mid 1 \leqslant i \leqslant n, \text{且 } G \cap F[x_{j_1}, \cdots, x_{j_i}] = G \cap F[x_{j_1}, \cdots, x_{j_{i-1}}]\}$$

是一个模于 I 的无关变元组. 此时, 若 x_k 是 $\overline{X} \backslash W$ 中最低的未定元, 则 $G \cap F[W, x_k] \neq \varnothing$.

证明 假若 W 模于 I 是相关的，则有非零 $h \in I \cap F[W]$. 由于 $h \in I$, 从而 h 可被 G 简化为零. 由文献 [22] 中定义 5.18 知，对于某个 $g \in G$, g 的首项 T 是 h 的某个非零项的因式. 此时必有， $T \in F[W]$. 用 m 表示最大的自然数，使得 x_{j_m} 在 T 中真正出现. 显然， $x_{j_m} \in W$, 即 $G \cap F[x_{j_1}, \cdots, x_{j_m}] = G \cap F[x_{j_1}, \cdots, x_{j_{m-1}}]$. 然而， $g \in G \cap F[x_{j_1}, \cdots, x_{j_m}]$, 但 $g \notin G \cap F[x_{j_1}, \cdots, x_{j_{m-1}}]$, 矛盾. 因此， W 模于 I 是无关的. 引理中后一叙述是显然的. 证毕.

根据引理 9.3.6, 对于 $F[\overline{X}]$ 的一个理想 I, 我们可以得到一个模于 I 的无关未定元组 W_1, 未定元 x_{k_1} 和一个非零 $g_{k_1} \in I \cap F[W_1, x_{k_1}]$. 如果 $\overline{X} = W_1 \cup \{x_{k_1}\}$, 则 W_1 是一个模于 I 的极大无关变元组. 否则，对于某个满足 $W_1 \prec \overline{X} \setminus (W_1 \cup \{x_{k_1}\}) \prec x_{k_1}$ 的字典序，再由引理 9.3.6 可得到未定元组 W_2 、未定元 x_{k_2} 和一个非零 $g_{k_2} \in I \cap F[W_2, x_{k_2}]$. 显然， $W_1 \subseteq W_2$. 如果 $\overline{X} = W_2 \cup \{x_{k_1}, x_{k_2}\}$, 则 W_2 是一个模于 I 的极大无关变元组. 否则, 对于某个满足 $W_2 \prec \overline{X} \setminus (W_2 \cup \{x_{k_1}, x_{k_2}\}) \prec x_{k_1} \prec x_{k_2}$ 的字典序, 由引理 9.3.6 又可得到未定元组 W_3 、未定元 x_{k_3} 和一个非零多项式 g_{k_3}, 使得

$W_2 \subseteq W_3$, 且 $g_{k_3} \in I \cap K[W_3, x_{k_3}]$. 如此进行下去，最后必得到未定元组 W_r, 未定元 x_{k_r} 和一个非零多项式 g_{k_r}, 使得 $\overline{X} = W_r \cup \{x_{k_1}, \cdots, x_{k_r}\}$, 且 $g_{k_r} \in I \cap F[W_r, x_{k_r}]$. 此时，$W_r$ 正是欲求的一个模于 I 的极大无关变元组. 此外，对于每个 $x \in \overline{X} \setminus W_r$, 我们都有非零多项式 g_x, 使得 $g_x \in I \cap F[W_r, x]$.

现设 D 是由非常量多项式组成的一个有限集合，满足：对于每个 $f \in D$, 存在 $s \in \{0, 1, \cdots, n-1\}$, 使得 f 是 $F_{\langle s\rangle}$ 上一个多项式，且在 f 中真正出现的未定元个数 $\leqslant n-s$. 同时，设 $\mathcal{E}$ 是由多项式组构成的有限集合，满足：对于每个 $E \in \mathcal{E}$, E 中含有有限个多项式，且存在 $s \in \{0, 1, \cdots, n-1\}$, 使得 E 中全部元素都是域 $F_{\langle s\rangle}$ 上多项式，且 $\dim(E) \leqslant n-s-1$.

对于如上的集合偶 $(D, \mathcal{E})$, 当 D 和 $\mathcal{E}$ 都是空集时，我们称答案为“错”. 当 D 和 $\mathcal{E}$ 不全为空集时，我们按如下两种方式之一执行操作.

方式一 $(D \neq \varnothing)$ 任取 $f \in D$. 通过“去偶因式”, 由 f 得到 f_1. 根据如下两种情况，分别进行操作：

情况 1 f_1 是一个单元多项式. 此时，用 Sturm 定理或定理 2.5.4 可确定 f_1 在 $R_{\langle n\rangle}$ 中是否有实根. 若 f_1 无实根，则令 $D^* = D \setminus \{f\}$, 且 $\mathcal{E}^* = \mathcal{E}$; 若 f_1 有实根，则停止下步操作，且称答案为“真”.

情况 2 $f_1 = f_1(x_{k_1}, \cdots, x_{k_r}) \in F_{\langle s\rangle}[x_{k_1}, \cdots, x_{k_r}]$, 这里 $1 < r \leqslant n-s$. 此时取

$$\begin{aligned} D^* = \ & (D \setminus \{f\}) \cup \{f_1(x_{k_1}, \cdots, x_{k_{r-1}}, 0)\} \\ & \cup \{f_1(x_{k_1}, \cdots, x_{k_{i-1}}, t_{s+1}^{-1}, x_{k_{i+1}}, \cdots, x_{k_r}) \mid i = 1, \cdots, r-1\} \\ & \cup \{f_1(x_{k_1}, \cdots, x_{k_{i-1}}, -t_{s+1}^{-1}, x_{k_{i+1}}, \cdots, x_{k_r}) \mid i = 1, \cdots, r-1\}; \end{aligned}$$

而取 $\mathcal{E}^* = \mathcal{E} \cup \{E\}$, 这里 $E = \{f_1 + \epsilon t_{s+1}, \dfrac{\partial f_1}{\partial x_{k_i}} \mid i = 1, \cdots, r-1\}$, 其中 ϵ 为 f_1 关于某个字典序的首项系数的符号.

方式二 $(\mathcal{E} \neq \varnothing)$ 任取 $E \in \mathcal{E}$. 设 E 所涉及的未定元组为 U, 且系数域为 $F_{\langle s\rangle}$. 计算 $F_{\langle s\rangle}[U]$ 中生成理想 $\mathrm{Id}(F)$ 的 Gröbner 基 G. 若 $1 \in G$, 则取 $D^* = D$, $\mathcal{E}^* = \mathcal{E} \setminus \{E\}$; 否则，按照引理 9.3.6 后的讨论，求出模于理想 $\mathrm{Id}(F)$ 的极大无关变元组 W 以及诸非零多项式 g_x $(x \in U \setminus W)$, 使得对于每个 $x \in U \setminus W$, $g_x \in \mathrm{Id}(F) \cap F_{\langle s\rangle}[W, x]$. 对于每个 $x \in U \setminus W$, 去 g_x 的重因式后得 ϕ_x. 令 $G_1 = E \cup \{\phi_x \mid x \in U \setminus W\}$. 根据文献 [22] 中引理 8.13 知，$G_1$ 在 $F_{\langle s\rangle}(W)[U \setminus W]$ 中生成的扩理想 I^e 是一个零维根理想. 设 $U \setminus W = \{x_{k_1}, \cdots, x_{k_r}\}$. 由文献 [22] 中定理 8.81 知，经过有限次试验后，可找到 $c_2, \cdots, c_r \in F$, 使得通过变量代换 π: $x_{k_1} \longmapsto x_{k_1} + c_2 x_{k_2} + \cdots + c_r x_{k_r}$, I^e 关于未定元 x_{k_1} 处于正规位置. 将 π 看作从 U 到自身的一个变量代换，且对于某个满足 $W \prec x_{k_1} \preceq U \setminus W$ 的字典序，计算理想 $\mathrm{Id}(\pi(G_1))$ 的 Gröbner 基 G_2. 在 G_2 中取出首项最低的元素 g, 并将 g 表为 $g = wh$, 其中 $w \in F_{\langle s\rangle}[W]$, h 是 $F_{\langle s\rangle}[W]$ 上含 x_{k_1} 的本原多项式. 然后，根据如下两种情况分别进行操作：

情况 1 $W=\phi$. 此时，h 是 $F_{\langle s\rangle}$ 上一个单元多项式. 若 h 在 $R_{\langle s\rangle}$ 中有实根，则称答案为“真”. 若 h 在 $R_{\langle s\rangle}$ 中无实根，则取 $D^*=D, \mathcal{E}^*=\mathcal{E}\setminus\{E\}$.

情况 2 $W\neq\phi$. 此时，取 $D^*=D\cup\{h\}, \mathcal{E}^*=(\mathcal{E}\setminus\{E\})\cup\{E_1,E_2\}$, 这里 $E_1=G_2\cup\{w\}, E_2=G_2\cup\{\dfrac{\partial h}{\partial y}\mid y=x_{k_1}$ 或 $y\in W\}$.

上述操作过程称作对 $(D,\mathcal{E})$ 的一个演绎，其输出是“真”、“错”或新的集合偶 $(D^*,\mathcal{E}^*)$. 容易看出，D^* 和 $\mathcal{E}^*$ 也满足对 D 和 $\mathcal{E}$ 所要求的有关条件，从而可再次对 $(D^*,\mathcal{E}^*)$ 进行如上演绎. 注意到，这样的演绎过程不可能无限地继续下去. 换句话说，通过有限次演绎后，可获得最终答案：“真”或“错”. 借助于定理 9.3.3 和定理 9.3.4, 容易证明如下命题.

命题 9.3.7 设集合偶 $(D,\mathcal{E})$ 同上，则经过有限次演绎后，可得到最终答案“真”或“错”, 且下列叙述成立：

(1) 当最终答案是“真”时，$\mathcal{E}$ 中至少有一个多项式组在 $R_{\langle n\rangle}$ 中有公共零点，或 D 中至少有一个多项式在 $R_{\langle n\rangle}$ 中不是半定的.

(2) 当最终答案是“错”时，$\mathcal{E}$ 中每个多项式组在 $R_{\langle n\rangle}$ 中没有公共零点，且 D 中每个多项式在 $R_{\langle n\rangle}$ 中是半定的.

由上面命题 9.3.7, 立即可以得到如下结果.

命题 9.3.8 设 $f\in F[X]$ 是一个非常量多项式，$D=\{f\}$, 且 $\mathcal{E}=\varnothing$, 则 f 在 R 中是半定的，当且仅当对 $(D,\mathcal{E})$ 进行有限次演绎后，所得的最终答案为“错”.

命题 9.3.9 设 $E=\{f_1,\cdots,f_r\}$ 是 $F[X]$ 的一个有限子集，其中 E 中元素不全为零，$D=\varnothing$, 且 $\mathcal{E}=\{E\}$, 则方程组 $f_i=0, i=1,\cdots,r$, 在 R 中有解，当且仅当对 $(D,\mathcal{E})$ 进行有限次演绎后，所得的最终答案为“真”.

作为上面结果的应用，我们借助于计算机代数系统 Maple V Release 4 来处理下面两个例子.

例 1 确定多项式 f 是否半定，这里 $f(x,y,z)=x^4+2x^2z+x^2-2xy+2y^2-2yz+2z^2-2x+2y+1$.

计算过程 根据命题 9.3.8, 我们进行如下 6 个演绎过程：

(1) 确定 $f_1=f(0,y,z)$ 是否半定. 为此，进行下面 4 个子过程：

(1.1) 考虑 $f_{11}=f(0,0,z)=2z^2+1$. 显然 f_{11} 无实根；

(1.2) 考虑 $f_{12}=f(0,y,t^{-1})=2y^2+(2-2t^{-1})y+2t^{-2}+1$. 由于判别式 $\Delta=-12t^{-2}+8t^{-1}-4<0$, 从而 f_{12} 无实根；

(1.3) 同子过程 (1.2), $f_{13}=f(0,y,-t^{-1})$ 也无实根；

(1.4) 考虑方程组 $f_{14}=\dfrac{\partial f_1}{\partial z}=0$, 这里 $f_{14}=f_1+t$. 通过计算，理想 $\mathrm{Id}\left(f_{14},\dfrac{\partial f_1}{\partial z}\right)$ 的 Gröbner 基为 $\{1\}$. 因此，该方程组无实解.

(2) 确定 $f_2 = f(x, t^{-1}, z)$ 是否半定. 为此, 进行下面 4 个子过程:

(2.1) 考虑 $f_{21} = f(0, t^{-1}, z) = 2z^2 - 2t^{-1}z + 2t^{-2} + 2t^{-1} + 1$. 由于判别式 $\Delta = -12t^{-2} - 16t^{-1} - 8 < 0$, 从而 f_{21} 无实根;

(2.2) 考虑 $f_{22} = f(x, t^{-1}, t_2^{-1}) = x^4 + (1 + t_2^{-1})x^2 - (2t^{-1} + 2)x + 2t^{-2} - 2t^{-1}t_2^{-1} + 2t_2^{-2} + 2t^{-1} + 1$. 计算多项式 f_{22} 的 Sylvester 矩阵的偶次顺序主子式, 获得该序列的符号表如下:

$$1, -1, 1, 1.$$

上面符号表的 (修订) 变号数为 2. 由定理 2.5.4 知, f_{22} 的实零点个数为 $4 - 2 \times 2 = 0$. 从而 f_{22} 无实根.

(2.3) 同子情况 (2.2), 可判定 $f_{23} = f(x, t^{-1}, -t_2^{-1})$ 也无实根;

(2.4) 考虑方程组 $f_{24} = \dfrac{\partial f_2}{\partial z} = 0$. 由计算, 生成理想 $(f_{24}, \frac{\partial f_2}{\partial z})$ 的 Gröbner 基为 $\{1\}$. 从而该方程组无实解.

由此可知, f_2 是半定的.

(3)~(5) 由类似过程 (2) 的计算可知, $f_3 = f(x, y, t^{-1})$, $f_4 = f(x, -t^{-1}, z)$ 和 $f_5 = f(x, y, -t^{-1})$ 都是半定的.

(6) 考虑方程组 $f_6 = \dfrac{\partial f}{\partial y} = \dfrac{\partial f}{\partial z} = 0$, 这里 $f_6 = f + t$. 通过计算知, 生成理想 $\left(f_6, \dfrac{\partial f}{\partial y}, \dfrac{\partial f}{\partial z}\right)$ 关于字典序 $z \prec y \prec x$ 的 Gröbner 基为 $\{g_1, g_2, g_3\}$, 其中 $g_3 = 9(z^2 + 3z + 1)^2 + 24tz^2 + 3t + 16t^2$. 由于 $t > 0$, 从而 g_3 无实根. 这样, 该方程组无实解.

因此, 根据命题 9.3.8, 多项式 f 是半 (正) 定的.

例 2 确定多项式组: $f_1 = f_2 = 0$ 是否有实解, 这里 $f_1 = 2x^2 - xy - 2y^2 - 2yz - z^2 - 1$, $f_2 = x^2 - xz + y^2 + yz + z^2 + 1$.

计算过程 通过计算知, 理想 $I = \mathrm{Id}(f_1, f_2)$ 关于字典序 $z \prec y \prec x$ 的 Gröbner 基为 $\{g_1, g_2, g_3, h\}$, 这里 $h = 17y^4 + 33y^3z + 37y^2z^2 + 25y^2 + 19yz^3 + 23yz + 7z^4 + 12z^2 + 9$. 由此可知, z 是模于 I 的一个极大无关未定元组. 计算 I 在 $\mathbb{Q}(z)[x, y]$ 中的拓展理想 I^e 关于字典序 $y \prec x$ 的 Gröbner 基如下:

$$G^e = \{(27z^2 + 3)x - 17y^3 - 67y^2z - (63z^2 + 13)y - 37z^3 - 37z,\ h\}.$$

这表明 I^e 关于变量 y 处于正规位置. 根据命题 9.3.9, 我们只须进行如下三个推理过程:

(1) 方程组 $f_1 = f_2 = u = 0$ 显然无解, 其中 $u = 1$ 是 h 作为 $\mathbb{Q}[z]$ 上含单变量 y 的多项式的所有系数的最大公因式.

(2) 考虑方程组 $f_1 = f_2 = \dfrac{\partial h}{\partial y} = \dfrac{\partial h}{\partial z} = 0$. 由计算知，理想 $\mathrm{Id}\left(f_1, f_2, \dfrac{\partial h}{\partial y}, \dfrac{\partial h}{\partial z}\right)$ 关于字典序 $z \prec y \prec x$ 的 Gröbner 基为

$$\{9x^2 - 9xz + 2,\ y - 2z,\ 1 + 9z^2\}.$$

由于 $1 + 9z^2$ 无实根，从而该方程组无实解.

(3) 判定 $h = h(y, z)$ 是否是半定的. 为此，进行如下子过程:

(3.1) 考虑 $h_1 = h(y, 0) = 17y^4 + 25y^2 + 9$. 显然， h_1 是半定的;

(3.2) 考虑 $h_2 = h(t^{-1}, z)$. 计算多项式 h_2 的 Sylvester 矩阵的偶次顺序主子式，获得该序列的符号表如下

$$1,\ -1,\ -1,\ 1.$$

上面符号表的 (修订) 变号数为 2. 由定理 2.5.4 知， h_2 的实零点个数为 $4 - 2 \times 2 = 0$. 从而， h_2 无实根;

(3.3) 同子过程 (3.2) 一样，可知 $h_3 = h(-t^{-1}, z)$ 也无实根;

(3.4) 考虑方程组 $h_4 = \dfrac{\partial h}{\partial y} = 0$, 这里 $h_4 = h + t$. 由计算知，生成理想 $(h_4, \dfrac{\partial h}{\partial y})$ 关于字典序 $z \prec y$ 的 Gröbner 基为 $\{1\}$. 因而，该方程组无实解.

根据命题 9.3.9 可知，所给的方程组 $f_1 = f_2 = 0$ 无实解.

§9.4　多项式理想的实根的计算

多项式理想的实根是实域论和实代数几何中一个重要的研究对象. 多项式理想的实根不仅在理论上有重要的研究价值，而且许多实际问题都可归结于多项式理想的实根的计算.

设 (F, P) 是一个序域， I 是多项式环 $F[\overline{X}] := F[x_1, \cdots, x_n]$ 的一个理想. 正如在定理 7.4.4 的推论 1 的证明中，我们可以得到 $F[\overline{X}]$ 的如下一个包含 I 的理想:

$$\sqrt[r]{I} := \{f \in F[\overline{X}] \mid \text{有}\xi_1, \cdots, \xi_m \in P\text{以及}g_1, \cdots g_m \in F[\overline{X}],\ \text{使得}f^{2k} + \sum_{i=1}^{m} \xi_i g_i^2 \in I,\ \text{其中}k \in \mathbb{N}\}.$$

上面的理想 $\sqrt[r]{I}$ 称作理想 I 的实根. 理想 I 称作是 $F[\overline{X}]$ 的一个实理想，若 $\sqrt[r]{I} = I$.

由实零点定理 (定理 7.4.4 的推论 1) 以及定理 7.4.4 的推论 2 可知，不仅可通过多项式理想的实根来判定多项式方程组是否有实解，而且可用于检验实多项式等式组之间的蕴含关系. 因此，有序几何中的许多自动推理问题都可演变成求多项式理想的实根以及检验相应的“成员”关系.

在本节中，始终设 $(F, \leqslant)$ 是一个可计算序域， P 是序 $\leqslant$ 的对应正锥，且 R 为

$(F,\leqslant)$ 的实闭包. 对于 $F[\overline{X}]$ 中一个子集 H, 仍用 $\mathrm{Id}(H)$ 表示 $F[\overline{X}]$ 中由子集 H 生成的理想. 此外, 假定域 F 具有一个分解单元多项式的有效算法. 从而域 F 具有一个分解多元多项式的有效算法 (参见文献 [197], §4.2 中定理 1). 作为一个熟知事实, 有理数域 $\mathbb{Q}$ 符合本节的要求.

为建立本节的主要结果, 我们需要准备一些引理.

引理 9.4.1 设 $(F,\leqslant)$ 和 $F[\overline{X}]$ 同上, (K,Q) 是序域 (F,P) 的一个序扩张, 且 J 是 $K[\overline{X}]$ 的一个实理想, 则 $J\cap F[\overline{X}]$ 是 $F[\overline{X}]$ 的一个实理想.

证明 由实理想的定义可知. 证毕.

引理 9.4.2 设 (F,P) 是一个序域, p 是 $F[\overline{X}]$ 中一个不可约多项式, 且 $\mathrm{Id}(p)$ 表示 $F[\overline{X}]$ 中由 p 生成的主理想, 则下列叙述等价:

(1) $\mathrm{Id}(p)$ 是 $F[\overline{X}]$ 的一个实理想;

(2) P 可拓展为 K 的一个正锥, 这里 K 是 $F[X]/\mathrm{Id}(p)$ 的分式域;

(3) p 在 (F,P) 的实闭包 R 上不是半定的.

证明 (1)$\Longrightarrow$(2): 由定理 1.1.2 知, 只须证明 T 是 K 的一个亚正锥, 这里 $T=\{\sum\limits_{i=1}^{m}c_ie_i^2\mid m\in\mathbb{N},\ \xi_i\in P\text{且}e_i\in K,\ i=1,\cdots,m\}$. 假若 $-1\in T$, 则 $1+\sum\limits_{i=1}^{m}\xi_ie_i^2=0$, 其中 $\xi_i\in P$ 且 $e_i\in K$, $i=1,\cdots,m$. 由 K 的构造, 有 $f,g_1,\cdots,g_m\in F[\overline{X}]$, 使得 $f\notin\mathrm{Id}(p)$, 且 $e_i=\dfrac{\overline{g_i}}{\overline{f}}$, 其中 $\overline{g_i}:=g_i+\mathrm{Id}(p)$, $\overline{f}:=f+\mathrm{Id}(p)\in F[\overline{X}]/\mathrm{Id}(p)\subseteq K, i=1,\cdots,m$. 由此有, $f^2+\sum\limits_{i=1}^{m}\xi_ig_i^2\in\mathrm{Id}(p)$. 由于 $\mathrm{Id}(p)$ 是一个实根理想, 从而 $f\in\mathrm{Id}(p)$, 矛盾. 因此, T 是 K 的一个亚正锥.

(2)$\Longrightarrow$(3): 设正锥 P 在 K 上有一个拓展 Q. 记 R_K 为 (K,Q) 的实闭包. 不失一般性, 假定变元 x_1 真正出现在多项式 p 中. 易见, $p(x_1,\overline{x_2},\cdots,\overline{x_n})$ 是 $K[x_1]$ 中一个不可约多项式, 其中 $\overline{x_i}:=x_i+\mathrm{Id}(p)\in K$, $i=2,\cdots,n$. 由于 $p(x_1,\overline{x_2},\cdots,\overline{x_n})$ 在 R_K 中有根 $\overline{x_1}$, 从而 $p(x_1,\overline{x_2},\cdots,\overline{x_n})$ 在 R_K 上不是半定的, 即 p 在 R_K 上不是半定的. 由转移定理 (定理 7.3.7) 可知, p 在 R 上不是半定的, 其中 R 是 (F,P) 的实闭包.

(3)$\Longrightarrow$(1): 设 p 在 R 上不是半定的, 其中 R 是 (F,P) 的实闭包. 显然, p 是 $F[x_1,\cdots,x_{n-1}]$ 上含 x_n 的一个本原多项式. 由引理 9.3.2 知, 有 $\eta_1,\cdots,\eta_n\in R_{\langle n\rangle}$, 使得 $p(\eta_1,\cdots,\eta_n)=0$, 且 $\eta_1,\cdots,\eta_{n-1}$ 在 F 上代数无关, 这里记号 $R_{\langle n\rangle}$ 的意义同引理 9.3.2.

设 $f^{2k}+\sum\limits_{i=1}^{m}\xi_ig_i^2\in\mathrm{Id}(p)$, 其中 $\xi_i\in P$, 而 $f,g_i\in F[\overline{X}]$, $i=1,\cdots,m$. 此时, 显然有

$$f^{2k}(\eta_1,\cdots,\eta_{n-1},\eta_n)+\sum_{i=1}^{m}\xi_i g_i^2(\eta_1,\cdots,\eta_{n-1},\eta_n)=0.$$

由此有 $f(\eta_1,\cdots,\eta_{n-1},\eta_n)=0$. 令 $g(y)=p(\eta_1,\cdots,\eta_{n-1},y)$. 显然，多项式 $g(y)$ 在域 $F(\eta_1,\cdots,\eta_{n-1})$ 上是不可约的. 从而，在多项式环 $F(\eta_1,\cdots,\eta_{n-1})[y]$ 中， $g(y)$ 是 $f(\eta_1,\cdots,\eta_{n-1},y)$ 的因式. 注意到 $\eta_1,\cdots,\eta_{n-1},y$ 在域 F 上是代数无关的，且 $g(y)$ 是 $F[\eta_1,\cdots,\eta_{n-1}]$ 上含 y 的本原多项式. 于是，在多项式环 $F[\eta_1,\cdots,\eta_{n-1},y]$ 中， $g(y)$ 是 $f(\eta_1,\cdots,\eta_{n-1},y)$ 的因式. 这意味着： $f\in \mathrm{Id}(p)$. 根据定义， $\mathrm{Id}(p)$ 是 $F[\overline{X}]$ 的一个实理想. 证毕.

引理 9.4.3 设 I 是 $F[\overline{X}]$ 的一个理想， $\{x_1,\cdots,x_m\}$ 是模于 I 的极大无关变元组，且记 I^e 为 I 在 $F(x_1,\cdots,x_m)[x_{m+1},\cdots,x_n]$ 上的扩理想. 如果 G 是 I 关于某个满足 $\{x_1,\cdots,x_m\}\prec x_{m+1}\prec\{x_{m+2},\cdots,x_n\}$ 的字典序的简化 Gröbner 基，那么 $I^e\cap F(x_1,\cdots,x_m)[x_{m+1}]$ 是由 g_{m+1} 生成的主理想，其中 g_{m+1} 是 G 中这样一个成员，其首项低于 G 中的其他成员.

证明 由于 $F(x_1,\cdots,x_m)[x_{m+1}]$ 是一个主理想整环，从而可设 h 为理想 $I^e\cap F(x_1,\cdots,x_m)[x_{m+1}]$ 的一个生成元. 由所设知， $I\cap F[x_1,\cdots,x_m,x_{m+1}]\neq\{0\}$, 因为 $\{x_1,\cdots,x_m\}$ 是模于 I 的极大无关变元组. 由文献 [22] 中命题 6.15 知, $G\cap F[x_1,\cdots,x_m,x_{m+1}]$ 是 $I\cap F[x_1,\cdots,x_m,x_{m+1}]$ 的一个 Gröbner 基. 因而, $G\cap F[x_1,\cdots,x_m,x_{m+1}]\neq\varnothing$. 由于 g_{m+1} 的首项在 G 的全部成员中是最低的，从而 $g_{m+1}\in F[x_1,\cdots,x_m,x_{m+1}]$. 必然，变元 x_{m+1} 真正出现在 g_{m+1} 中.

注意到 $g_{m+1}\in G\cap F[x_1,\cdots,x_m,x_{m+1}]\subseteq I^e\cap F(x_1,\cdots,x_m)[x_{m+1}]$, 我们有 $g_{m+1}=uh$, 对于某个 $u\in F(x_1,\cdots,x_m)[x_{m+1}]$. 因而， $h\neq 0$ 且 $\deg(h;x_{m+1})\leqslant\deg(g_{m+1};x_{m+1})$, 其中 $\deg(h;x_{m+1})$ 和 $\deg(g_{m+1};x_{m+1})$ 分别表示 h 和 g_{m+1} 关于变元 x_{m+1} 的次数. 由 I^e 的构造，有非零的 $w\in F[x_1,\cdots,x_m]$, 使得 $wh\in I$. 因而，模于 Gröbner 基 G, wh 可以被简化为 0. 假若 $\deg(h;x_{m+1})<\deg(g_{m+1};x_{m+1})$, 则 $\deg(wh;x_{m+1})<\deg(g_{m+1};x_{m+1})$. 易知， wh 的首项低于 g_{m+1}, 因而低于 G 中每个成员. 根据文献 [22] 中定义 5.18 知， wh 是模于 G 的一个规范形，矛盾. 从而 $\deg(h;x_{m+1})=\deg(g_{m+1};x_{m+1})$. 这表明. h 和 g_{m+1} 在 $F(x_1,\cdots,x_m)[x_{m+1}]$ 中是相伴的. 因此， g_{m+1} 也是理想 $I^e\cap F(x_1,\cdots,x_m)[x_{m+1}]$ 的一个生成元. 证毕.

引理 9.4.4 设 I 是 $F[\overline{X}]$ 的一个理想， $\{x_1,\cdots,x_m\}$ 是模于 I 的极大无关变元组，且 G 是 I 关于某个满足 $\{x_1,\cdots,x_m\}\prec x_{m+1}\prec x_{m+2}\prec\cdots\prec x_n$ 的字典序的简化 Gröbner 基. 若 I 在 $F(x_1,\cdots,x_m)[x_{m+1},\cdots,x_n]$ 中的扩理想 I^e 是 $F(x_1,\cdots,x_m)[x_{m+1},\cdots,x_n]$ 的一个根理想，则 I^e 关于 x_{m+1} 处于正规位置，当且仅当对于 $k=m+2,\cdots,n$, 存在一个 $g_k\in G$, 使得 $g_k=u_kx_k+v_k$, 其中 u_k 是 $F[x_1,\cdots,x_m]$ 中非零多项式，且 $v_k\in F[x_1,\cdots,x_{k-1}]$.

证明 充分性：设 $g_k=u_kx_k+v_k\in G$, 其中 u_k 是 $F[x_1,\cdots,x_m]$ 中非零多

项式，且 $v_k \in F[x_1, \cdots, x_{k-1}]$, $k = m+2, \cdots, n$. 记 Ω 为域 $F(x_1, \cdots, x_m)$ 的代数闭包. 显然, $g_k \in I^e$, $k = m+2, \cdots, n$. 因而，对于 I^e 在 Ω 中的任意零点 $(\eta_{m+1}, \cdots, \eta_n)$, 有 $u_k\eta_k - v_k(\eta_{m+1}, \cdots, \eta_{k-1}) = 0$, 即 $\eta_k = u_k^{-1}v_k(\eta_{m+1}, \cdots, \eta_{k-1})$, $k = m+2, \cdots, n$. 因而, $\eta_{m+2}, \cdots, \eta_n$ 都是由 η_{m+1} 惟一确定的. 根据文献 [22] 中定义 8.67 知, I^e 关于变元 x_{m+1} 处于正规位置.

必要性: 设 I^e 关于变元 x_{m+1} 处于正规位置. 显然, I^e 是一个零维理想. 由文献 [22] 中命题 8.77 知，关于任意一个满足 $x_{m+1} \prec \{x_{m+2}, \cdots, x_n\}$ 的字典序, I^e 的简化 Gröbner 基 G^e 具有如下形式:

$$G^e = \{h_{m+1}, x_{m+2} - h_{m+2}, \cdots, x_n - h_n\},$$

其中 $h_k \in F(x_1, \cdots, x_m)[x_{m+1}]$, $k = m+1, \cdots, n$.

由 I^e 的结构知，有非零的 $w_k \in F[x_1, \cdots, x_m]$, 使得 $w_k(x_k - h_k) \in I$, $k = m+2, \cdots, n$. 由 [22] 中的命题 5.38 知, $w_k(x_k - h_k)$ 模于 G 是首位可约的, $k = m+2, \cdots, n$. 注意到 $w_k(x_k - h_k)$ 的首项式是 $w_k'x_k$, 其中 w_k' 是 w_k 的首项式, $k = m+2, \cdots, n$. 因而，存在 $g_k \in G$, 使得 g_k 的首项式 $HM(g_k)$ 整除 $w_k'x_k$, 且 $e_k := w_k(x_k - h_k) - \dfrac{w_k'x_k}{HM(g_k)}g_k \in I \cap F[x_1, \cdots, x_{k-1}]$, $k = m+2, \cdots, n$. 假若变元 x_j 不出现在 g_j 的首项，其中 $j \in \{m+2, \cdots, n\}$, 则 $g_j \in F[x_1, \cdots, x_{j-1}]$. 记 $G_0 := G^e \cap F(x_1, \cdots, x_m)[x_{m+1}, \cdots, x_{j-1}]$, 则有

$$G_0 = \{h_{m+1}, x_{m+2} - h_{m+1}, \cdots, x_{j-1} - h_{j-1}\}.$$

由 [22] 中命题 6.15 知, G_0 是 $I^e \cap F(x_1, \cdots, x_m)[x_{m+1}, \cdots, x_{j-1}]$ 的简化 Gröbner 基. 显然, $e_j, g_j \in I^e \cap F(x_1, \cdots, x_m)[x_{m+1}, \cdots, x_{j-1}]$. 因而, g_j 模于 G_0 是可约的. 由等式 $x_j - h_j = w_j^{-1}(\frac{w_j'x_j}{HM(g_j)}g_j + e_j)$ 可见，作为 $F(x_1, \cdots, x_m)[x_{m+1}, \cdots, x_n]$ 中一个元素, $x_j - h_j$ 模于 G_0 是可约的. 这矛盾于事实: I^e 的 Gröbner 基 G^e 是简化的. 因而，变元 x_k 真正出现在 g_k 的首项, $k = m+2, \cdots, n$. 此时, g_k 必可表为 $g_k = u_kx_k + v_k$, 其中 u_k 为 $F[x_1, \cdots, x_m]$ 中非零元，且 $v_k \in F[x_1, \cdots, x_{k-1}]$, $k = m+2, \cdots, n$. 证毕.

引理 9.4.5 设 $H \subseteq F[X]$, I 是 $F[X]$ 中由 H 生成的理想, $\{x_1, \cdots, x_m\}$ 是模于 I 的一个极大无关变元组，且 I^e 是 I 在 $F(x_1, \cdots, x_m)[x_{m+1}, \cdots, x_n]$ 上的扩理想. 如果对于 $k = m+2, \cdots, n$, 有 $g_k \in H$, 使得 $g_k = u_kx_k + v_k$, 其中 u_k 是 $F[x_1, \cdots, x_m]$ 中非零元，且 $v_k \in F[x_1, \cdots, x_{k-1}]$, 那么 $\{g_{m+1}, g_{m+2}, \cdots, g_n\}$ 是 I^e 的一个 Gröbner 基，其中 g_{m+1} 是主理想 $I^e \cap F(x_1, \cdots, x_m)[x_{m+1}]$ 的一个生成元.

证明 记 J 为 $F(x_1, \cdots, x_m)[x_{m+1}, \cdots, x_n]$ 中由 $\{g_{m+1}, g_{m+2}, \cdots, g_n\}$ 生成的理想. 显然, $J \subseteq I^e$. 由 [22] 中定理 5.68 知, $\{g_{m+1}, g_{m+2}, \cdots, g_n\}$ 是 J 的一个 Gröbner 基，因为 $\{g_{m+1}, g_{m+2}, \cdots, g_n\}$ 中任意两个成员的首项是不相交的. 对于

任意 $\phi\in I^e$, 通过相继地用 $g_n,\cdots,g_{m+2}$ 除 ϕ, 可得如下等式:

$$\phi=q_ng_n+\cdots+q_{m+2}g_{m+2}+r,$$

其中 $r\in F(x_1,\cdots,x_m)[x_{m+1}]$, 且 $q_k\in F(x_1,\cdots,x_m)[x_{m+1},\cdots,x_k]$, $k=m+2,\cdots,n$. 显然 $r\in I^e\cap F(x_1,\cdots,x_m)[x_{m+1}]$, 即有 $r=q_{m+1}g_{m+1}$, 这里 $q_{m+1}\in K(x_1,\cdots,x_m)[x_{m+1}]$. 因而 $\phi\in J$, 即有 $I^e=J$. 证毕.

引理 9.4.6 设 J 是 $F(x_1,\cdots,x_m)[x_{m+1},\cdots,x_n]$ 中由如下子集生成的理想:

$$\{g_{m+1},u_{m+1}x_{m+2}-v_{m+2},\cdots,u_nx_n-v_n\},$$

其中 g_{m+1} 是 $F[x_1,\cdots,x_{m+1}]$ 中一个不可约多项式, u_k 是 $F[x_1,\cdots,x_m]$ 中非零元, 且 $v_k\in F[x_1,\cdots,x_{k-1}]$, $k=m+2,\cdots,n$. 若 g_{m+1} 在 (F,P) 的实闭包上不是半定的, 且变元 x_{m+1} 真正出现在 g_{m+1} 中, 则对于正锥 P 在 $F(x_1,\cdots,x_m)$ 的某个拓展, J 是 $F(x_1,\cdots,x_m)[x_{m+1},\cdots,x_n]$ 的一个实素理想.

证明 记 K 为 $F[x_1,\cdots,x_{m+1}]/\mathrm{Id}(g_{m+1})$ 的分式域, 且用 η_{m+1} 表示 K 中元 $x_{m+1}+\mathrm{Id}(g_{m+1})$. 由引理 9.4.2, P 在 K 上有一个拓展 Q_K. 很清楚, $F[x_1,\cdots,x_m]\cap\mathrm{Id}(g_{m+1})=\{0\}$. 从而有

$$F[x_1,\cdots,x_m]+\mathrm{Id}(g_{m+1})/\mathrm{Id}(g_{m+1})\cong F[x_1,\cdots,x_m].$$

因而, $F[x_1,\cdots,x_m]$ 可看作 $K[x_1,\cdots,x_{m+1}]/\mathrm{Id}(g_{m+1})$ 的一个子环. 于是, 可认定 $F(x_1,\cdots,x_m)\subseteq K$. 令 $Q=Q_K\cap F(x_1,\cdots,x_m)$, 则 Q 是 P 在 $F(x_1,\cdots,x_m)$ 上的一个拓展.

将 v_k 看作域 K 上含变元 $x_{m+1},\cdots,x_{k-1}$ 的多项式, 且递归地定义 η_k, 使得

$$\eta_k=u_k^{-1}v_k(\eta_{m+1},\cdots,\eta_{k-1}),\ k=m+2,\cdots,n.$$

显然, 存在 $F(x_1,\cdots,x_m)[x_{m+1},\cdots,x_n]$ 到 K 中的一个 $F(x_1,\cdots,x_m)$- 同态 π, 使得 $\pi(x_k)=\eta_k$, $k=m+1,\cdots,n$. 此时, $J\subseteq\ker(\pi)$. 另一方面, 对于任意 $\phi\in\ker(\pi)$, 相继地用 $u_nx_n-v_n,\cdots,u_{m+2}x_{m+2}-v_{m+2}$ 除 ϕ 可得, $\phi=q_n(u_nx_n-v_n)+\cdots+q_{m+2}(u_{m+1}x_{m+1}-v_{m+2})+r$, 其中 $r\in F(x_1,\cdots,x_m)[x_{m+1}]$, 且 $q_k\in F(x_1,\cdots,x_m)[x_{m+1},\cdots,x_k]$, $k=m+2,\cdots,n$. 通过代换 $x_k=\eta_k$, $k=m+1,\cdots,n$, 有 $r(\eta_{m+1})=0$. 从而有某个 $q_{m+1}\in F(x_1,\cdots,x_m)[x_{m+1}]$, 使得 $r=q_{m+1}g_{m+1}$. 于是 $\phi\in J$, 即有 $\ker(\pi)=J$. 因而, $F(x_1,\cdots,x_m)[x_{m+1},\cdots,x_n]/J$ 同构于 K 的一个子环. 从而 J 是 $F(x_1,\cdots,x_m)[x_{m+1},\cdots,x_n]$ 的一个素理想.

设 $f^{2k}+\sum\limits_{i=1}^{s}\xi_ih_i^2\in J$, 其中 $s\in\mathbb{N}$, f, $h_i\in F(x_1,\cdots,x_m)[x_{m+1},\cdots,x_n]$, $\xi_i\in Q$, $i=1,\cdots,s$. 在同态 π 的作用下, 我们有关于 K 中元素的如下等式:

$$\pi(f)^{2k}+\sum_{i=1}^{s}\xi_i\pi(h_i)^2=0.$$

由此可知, $\pi(f)=0$, 即 $f\in\ker(\pi)=J$. 因此, 对于 P 在 $F(x_1,\cdots,x_m)$ 的拓展 Q, J 是一个实理想. 证毕.

根据上面诸引理, 现在我们可以着手考虑多项式理想的实根的计算问题.

设 I 是 $F[\overline{X}]$ 的一个由有限子集 H 生成的真理想. 对此, 我们有效地进行如下运算:

(1) 对于任意一个字典序, 计算 I 的一个 Gröbner 基 G. 根据引理 9.3.6, 求出模于 I 的一个极大无关变元组 S.

(2) 对于每个 $x\in\overline{X}\setminus S$, 关于某个满足 $S\prec x\preceq\overline{X}\setminus S$ 的字典序, 计算 I 的一个 Gröbner 基 G_x, 且找出 G_x 中首项最低的成员 g_x. (由引理 9.4.3 知, $g_x\in F[S,x]$, 但 $g_x\notin F[S]$.)

此外, 计算出每个 g_x 的无平方部分 h_x, 且令 $G_1:=G\cup\{h_x\mid x\in\overline{X}\setminus S\}$. (此时, 由 [22] 中引理 8.13 知, I^e 是 $F(S)[\overline{X}\setminus S]$ 的一个零维根理想, 其中 I^e 是 $\mathrm{Id}(G_1)$ 在 $F(S)[X\setminus S]$ 上的扩理想.)

(3) 假定 $\overline{X}\setminus S=\{x_{k_1},\cdots,x_{k_m}\}$. (根据 [22] 中定理 8.81, 通过有限次测试, 可找到 $c_2,\cdots,c_m\in F$, 使得经过变换 π: $x_{k_1}\longrightarrow x_{k_1}+c_2x_{k_2}+\cdots+c_mx_{k_m}$, I^e 关于变元 x_{k_1} 处于正规位置.) 鉴于引理 9.4.4, 可找到 $c_2,\cdots,c_m\in K$ 和相应的变换 π, 使得 $\mathrm{Id}(\pi(G_1))$ 关于任意一个满足 $S\prec x_{k_1}\preceq\overline{X}\setminus S$ 的字典序的 Gröbner 基 G_2 包含如下形式的成员:

$$g_{k_i}=u_ix_{k_i}-v_i,\ i=2,\cdots,m,$$

其中 u_i 是 $F[S]$ 中非零元, 且 $v_i\in F[S,x_{k_1},\cdots,x_{k_{i-1}}]$, $i=2,\cdots,m$.

(4) 找出 G_2 中首项最低的成员 g_1. (由引理 9.4.3 知, $g_1\in F[S,x_{k_1}]$.) 同时将 g_1 分解成不可约因式之积 $g_1=w_1\cdots w_rp_1\cdots p_s$, 其中 $w_j\in F[S]$, $j=1,\cdots,r$, 且 $p_k\in F[S,x_{k_1}]$, $k=1,\cdots,s$.

(5) 对于 $k=1,\cdots,s$, 判定 p_k 在 (F,P) 的实闭包 R 上是否为半定的. 设 $p_1,\cdots,p_t$ 在 (F,P) 的实闭包 R 上是半定的, 但 $p_{t+1},\cdots,p_s$ 在 R 上不是半定的, 其中 $0\leqslant t\leqslant s$.

(6) 构造 $F[\overline{X}]$ 的如下新理想:

(6.1) 对于 $j=1,\cdots,r$, 令 $I_j=\mathrm{Id}(G_2\cup\{w_j\})$;

(6.2) 对于 $k=1,\cdots,t$, 令 $J_k=\mathrm{Id}\left(G_2\cup\left\{\dfrac{\partial p_k}{\partial x}\mid x\in S\text{或}x=x_{k_1}\right\}\right)$;

(6.3) 记 $\Lambda=\{i\mid 2\leqslant i\leqslant m,\text{且}u_i\notin F\}$; 对于 $\lambda\in\Lambda$, 令 $L_\lambda=\mathrm{Id}(G_2\cup\{u_\lambda\})$.

(6.4) 对于 $k=t+1,\cdots,s$, 令 $E_k=\mathrm{Id}(G_2\cup\{p_k\})$. 并根据 [22] 中命题 6.37 或

推论 6.36, 计算出理想 D_k, 使得 $D_k = Q_k : u^\infty$, 其中 u 是 $u_2, \cdots, u_r$ 的最小公倍式.

为叙述方便，上面的全过程称作对 I 的一次 π- 化简. 由 (6.1), (6.2) 和 (6.3) 所得的新理想都称作未确定的输出理想，而由 (6.4) 所得的新理想都称作确定的输出理想.

注 若 J 是如上所得的一个未确定的输出理想，则 $F[\overline{X}]$ 中有这样一个严格的理想升链 $I = \mathrm{Id}(H) \subset \pi^{-1}(J)$, 其中 π^{-1} 是 π 的逆变换: $x_{k_1} \longmapsto x_{k_1} - c_2 x_{k_2} - \cdots - c_m x_{k_m}$.

现在，我们可以建立如下主要结论.

定理 9.4.7 设记号同上，则有

$$\sqrt[r]{\pi(I)} = \left(\bigcap_{j=1}^{r} \sqrt[r]{I_j}\right) \cap \left(\bigcap_{k=1}^{t} \sqrt[r]{J_k}\right) \cap \left(\bigcap_{\lambda\in\Lambda} \sqrt[r]{L_\lambda}\right) \cap \left(\bigcap_{k=t+1}^{s} D_k\right).$$

证明 首先，我们证明下面三个断言.

断言 1 $\sqrt[r]{\pi(I)} = \left(\bigcap_{j=1}^{r} \sqrt[r]{I_j}\right) \cap \left(\bigcap_{k=1}^{t} \sqrt[r]{J_k}\right) \cap \left(\bigcap_{k=t+1}^{s} \sqrt[r]{E_k}\right)$.

显然，$\pi(I) \subseteq \mathrm{Id}(G_2) \subseteq \left(\bigcap_{j=1}^{r} I_j\right) \cap \left(\bigcap_{k=1}^{t} J_k\right) \cap \left(\bigcap_{k=t+1}^{s} E_k\right)$. 因而有

$$\begin{aligned}\sqrt[r]{\pi(I)} &\subseteq \sqrt[r]{\left(\bigcap_{j=1}^{r} I_j\right) \cap \left(\bigcap_{k=1}^{t} J_k\right) \cap \left(\bigcap_{k=t+1}^{s} E_k\right)} \\ &= \left(\bigcap_{j=1}^{r} \sqrt[r]{I_j}\right) \cap \left(\bigcap_{k=1}^{t} \sqrt[r]{J_k}\right) \cap \left(\bigcap_{k=t+1}^{s} \sqrt[r]{E_k}\right).\end{aligned}$$

设 R 是 (F,P) 的实闭包，且 $\alpha \in R^n$, 使得对于每个 $h \in \pi(I)$, $h(\alpha) = 0$. 由 G_2 的构造知，对于每个 $g \in G_2$, $g(\alpha) = 0$. 因而， $g_1(\alpha) = 0$. 从而，对于某个 $j_0 \in \{1, \cdots, r\}$, $w_{j_0}(\alpha) = 0$; 或者对于某个 $k_0 \in \{1, \cdots, s\}$, $p_{k_0}(\alpha) = 0$. 对于任意 $f \in \left(\bigcap_{j=1}^{r} I_j\right) \cap \left(\bigcap_{k=1}^{t} J_k\right) \cap \left(\bigcap_{k=t+1}^{s} E_k\right)$, 考虑如下可能情形:

情形 1 对于某个 $j_0 \in \{1, \cdots, r\}$, $w_{j_0}(\alpha) = 0$. 此时，由于 $f \in I_{j_0} = \mathrm{Id}(G_2 \cup \{w_{j_0}\})$, 从而 $f(\alpha) = 0$.

情形 2 $p_{k_0}(\alpha) = 0$ 且 $1 \leqslant k_0 \leqslant t$. 由于 p_{k_0} 在 R 上是半定的, 从而对于每个 $x \in S \cup \{x_{k_1}\}$, $\dfrac{\partial p_{k_0}}{\partial x}(\alpha) = 0$. 此时, 由于 $f \in J_{k_0} = \mathrm{Id}\left(G_2 \cup \left\{\dfrac{\partial p_{k_0}}{\partial x} \mid x \in S \text{或} x = x_{k_1}\right\}\right)$, 从而 $f(\alpha) = 0$.

情形 3 $p_{k_0}(\alpha) = 0$ 且 $t+1 \leqslant k_0 \leqslant s$. 此时，由于 $f \in E_{k_0} = \mathrm{Id}(G_2 \cup \{p_{k_0}\})$,

从而 $f(\alpha)=0$.

由实零点定理知, $f\in\sqrt[r]{\pi(I)}$. 从而 $\left(\bigcap_{j=1}^{r}I_j\right)\cap\left(\bigcap_{k=1}^{t}J_k\right)\cap\left(\bigcap_{k=t+1}^{s}E_k\right)\subseteq\sqrt[r]{\pi(I)}$. 于是 $\left(\bigcap_{j=1}^{r}\sqrt[r]{I_j}\right)\cap\left(\bigcap_{k=1}^{t}\sqrt[r]{J_k}\right)\cap\left(\bigcap_{k=t+1}^{s}\sqrt[r]{E_k}\right)\subseteq\sqrt[r]{\sqrt[r]{\pi(I)}}=\sqrt[r]{\pi(I)}$. 因而, 断言 1 成立.

断言 2 $\left(\bigcap_{\lambda\in\Lambda}\sqrt[r]{L_\lambda}\right)\cap\sqrt[r]{D_k}\subseteq\sqrt[r]{E_k}$, $k=t+1,\cdots,s$.

设 R 是 (F,P) 的实闭包, 且 $\alpha\in R^n$, 使得对于每个 $h\in E_k$, $h(\alpha)=0$. 对于任意 $f\in\left(\bigcap_{\lambda\in\Lambda}L_\lambda\right)\cap D_k$, $f\in D_k=E_k:u^\infty$, 即有 $\varepsilon\in\mathbb{N}$, 使得 $u^\varepsilon f\in E_k$. 于是 $u(\alpha)^\varepsilon f(\alpha)=0$. 从而 $f(\alpha)=0$ 或 $u(\alpha)=0$. 当 $u(\alpha)=0$ 时, 由于 u 是 Λ 中全部成员的最小公倍式, 从而必有某个 $\lambda\in\Lambda$, 使得 $u_\lambda(\alpha)=0$. 由于 $f\in L_\lambda=\mathrm{Id}(G_2\cup\{u_\lambda\})$, 从而仍有 $f(\alpha)=0$. 由实零点定理知, $f\in\sqrt[r]{E_k}$. 从而, $\left(\bigcap_{\lambda\in\Lambda}L_\lambda\right)\cap D_k\subseteq\sqrt[r]{E_k}$. 因此, 断言 2 成立.

断言 3 D_k 是 $F[\overline{X}]$ 的一个实素理想, $k=t+1,\cdots,s$.

用 E_k^e 表示 E_k 在 $F(S)[X\setminus S]$ 上的扩理想. 假若 $1\in E_k^e$, 则有某个非零的 $w\in F[S]$, 使得 $w\in E_k$. 令 $h:=w_1\cdots w_r p_1\cdots p_{k-1}wp_{k+1}\cdots p_s$. 很清楚, $h\in I_1\cdots I_r\cdot\mathrm{Id}(G_2\cup\{p_1\})\cdots\mathrm{Id}(G_2\cup\{p_s\})\subseteq\mathrm{Id}(G_2)$. 因而, h 模于 G_2 是首位可简化的. 然而 h 的首项低于 g_1, 自然低于 G_2 中每个成员, 矛盾. 因而, $1\notin E_k^e$, 即 $E_k^e\cap F(S)[x_{k_1}]$ 是 $F(S)[x_{k_1}]$ 的一个真理想. 注意到 p_k 在 $F(S)[x_{k_1}]$ 中是不可约的, 且 $p_k\in E_k^e\cap F(S)[x_{k_1}]$. 因而, $E_k^e\cap F(S)[x_{k_1}]$ 是 $F(S)[x_{k_1}]$ 中由 p_k 生成的主理想. 由引理 9.4.5, $\{p_k,g_{k_2},\cdots,g_{k_m}\}$ 是 E_k^e 的一个 Gröbner 基. 由引理 9.4.6, E_k^e 是 $F(S)[X\setminus S]$ 的一个实素理想.

很清楚, $p_k\in E_k^e\cap F[\overline{X}]$. 对于任意 $\phi\in E_k^e\cap F[\overline{X}]$, 相继地用 $g_{k_m},\cdots,g_{k_2}$ 除 ϕ 可得

$$u^\ell\phi=q_m g_{k_m}+\cdots+q_2g_{k_2}+\mu,$$

其中 $\ell\in\mathbb{N}$, $\mu\in F[S,x_{k_1}]$, 且 $q_i\in F[S,x_{k_1},\cdots,x_{k_i}]$, $i=2,\cdots,m$. 显然, $\mu\in E_k^e\cap F(S)[x_{k_1}]$. 因而, 在 $F(S)[x_{k_1}]$ 中 p_k 整除 μ. 注意到 $F[S]$ 是一个惟一分解整环, 且 p_k 是 $F[S]$ 上一个本原的单元多项式. 由熟知的 Gauss 引理易见, 存在 $q_1\in F[S,x_{k_1}]$, 使得 $\mu=q_1p_k$. 于是 $u^\ell\phi\in E_k$, 即 $\phi\in E_k:u^\infty=D_k$. 因而, $E_k^e\cap F[\overline{X}]=D_k$. 根据引理 9.4.1, D_k 是 $F[\overline{X}]$ 的一个实素理想.

由上面的断言, 立即可推出

$$\left(\bigcap_{j=1}^{r}\sqrt[r]{I_j}\right)\cap\left(\bigcap_{k=1}^{t}\sqrt[r]{J_k}\right)\cap\left(\bigcap_{\lambda\in\Lambda}\sqrt[r]{L_\lambda}\right)\cap\left(\bigcap_{k=t+1}^{s}D_k\right)\subseteq\sqrt[r]{\pi(I)}.$$

此外，显然有

$$\pi(I) \subseteq \left(\bigcap_{j=1}^{r} I_j\right) \cap \left(\bigcap_{k=1}^{t} J_k\right) \cap \left(\bigcap_{\lambda\in\Lambda} L_\lambda\right) \cap \left(\bigcap_{k=t+1}^{s} D_k\right).$$

于是有

$$\begin{aligned}\sqrt[r]{\pi(I)} &\subseteq \sqrt[r]{\left(\bigcap_{j=1}^{r} I_j\right) \cap \left(\bigcap_{k=1}^{t} J_k\right) \cap \left(\bigcap_{\lambda\in\Lambda} L_\lambda\right) \cap \left(\bigcap_{k=t+1}^{s} D_k\right)} \\ &= \left(\bigcap_{j=1}^{r} \sqrt[r]{I_j}\right) \cap \left(\bigcap_{k=1}^{t} \sqrt[r]{J_k}\right) \cap \left(\bigcap_{\lambda\in\Lambda} \sqrt[r]{L_\lambda}\right) \cap \left(\bigcap_{k=t+1}^{s} D_k\right).\end{aligned}$$

证毕.

定理 9.4.8 设 I 是 $F[\overline{X}]$ 中一个由有限子集 H 生成的理想，则通过有限次化简后，可计算出 I 的实根 $\sqrt[r]{I}$, 使得 $\sqrt[r]{I}$ 被表示为有限个实素理想的交.

证明 我们的计算过程如下.

作为始步，计算 I 关于任意字典序的一个 Gröbner 基 G. 若 $F\cap G\neq\emptyset$, 则终止计算，而获得浅显结果 $\sqrt[r]{I}=\mathrm{Id}(1)$. 当 $F\cap G=\emptyset$, 即 I 是 $F[\overline{X}]$ 的一个真理想，我们将执行对 I 的第一次化简. 若每个输出理想是确定的或浅显的，我们的计算终止. 否则，我们对每个未确定的输出理想再次执行化简. 一般说来，在执行一次化简后，若每个输出理想是确定的或浅显的，则计算终止. 否则，我们对每个未确定的输出理想再次执行化简.

假若我们的化简会无休止地进行下去，则由上面的附注可知，将获得 $F[\overline{X}]$ 中一个由无限多个理想组成的严格升链. 这是不可能的，因为 $F[\overline{X}]$ 是一个 Noether 环. 因而，我们的化简必在有限次后终止. 换句话说，在有限次化简后，所得的输出理想都是确定的或浅显的.

记 $\mathcal{D}$ 为整个化简过程中所得的全部确定的输出理想. 对于每个 $D\in\mathcal{D}$, 用 π_D 表示在由 I 简化到 D 的过程中所有变元变换的乘积. 由定理 9.4.7 可知，$\sqrt[r]{I}=\bigcap_{D\in\mathcal{D}}\pi_D^{-1}(D)$, 其中 $\pi_D^{-1}(D)$ 是 $F[\overline{X}]$ 的一个实素理想. 证毕.

作为上面定理的一个应用，我们用软件 Maple 来处理如下实例.

例 设 $\mathbb{Q}[x,y,z]$ 是有理数域 $\mathbb{Q}$ 上多项式环，$f_1=(x^2-z^3+z^2)(z^2-1)$, $f_2=x(x^2-z^3+z^2)$, 且 $f_3=x-y^2+z$. 计算理想 I 的实根，其中 I 是 $\mathbb{Q}[x,y,z]$ 中由 f_1, f_2 和 f_3 生成的理想.

计算过程 根据定理 9.4.7 及其证明，我们进行如下计算.

(1) 执行如下一次对 I 的化简：

(1.1) 对于满足 $z\prec y\prec x$ 的字典序，计算出 I 的简化 Gröbner 基 G 如下：

$$G = \{x - y^2 + z,\ y^6 - 3zy^4 - z^3y^2 + 4z^2y^2 + z^4 - 2z^3,$$
$$z^2y^4 - y^4 - 2z^3y^2 + 2zy^2 - z^5 + 2z^4 + z^3 - 2z^2\}.$$

根据引理 9.3.6 可知， $\{z\}$ 是模于 I 的极大无关变元组.

(1.2), (1.3) 注意到 $g_1 := x - y^2 + z \in G$. 由引理 9.4.4 知， I 在 $\mathbb{Q}(z)[x, y]$ 上的扩理想 I^e 关于变元 y 处于正规位置.

(1.4) 在 G 中, 首项最低的成员是 $g_2 := z^2y^4 - y^4 - 2z^3y^2 + 2zy^2 - z^5 + 2z^4 + z^3 - 2z^2$. 分解 g_2 为不可约因式的乘积 $g_2 = (z-1)(z+1)p(y, z)$, 其中 $p(y, z) = y^4 - 2zy^2 - z^3 + 2z^2$.

(1.5), (1.6) 注意到， g_1 作为一个含 x 的单元多项式，它的首项为 1. 因而，我们获得如下两个未确定的输出理想:

$$I_1 = \mathrm{Id}(G \cup \{z - 1\}), \qquad I_2 = \mathrm{Id}(G \cup \{z + 1\}).$$

显然， $p(0, z) = -z^3 + 2z^2$ 不是半定的. 因而， $p(y, z)$ 不是半定的. 令 $E = \mathrm{Id}(G \cup \{p(y, z)\}) = \mathrm{Id}(g_1, p(y, z))$, 则得确定的输出理想 $D_1 = E : 1 = E$.

(2) 执行一次对 I_1 的如下化简:

(2.1) 对于满足 $z \prec y \prec x$ 的字典序，计算出 I_1 的简化 Gröbner 基 G_1 如下:

$$G_1 = \{x - y^2 + 1, y^6 - 3y^4 + 3y^2 - 1, z - 1\}.$$

(2.2), (2.3) 由 [22] 中定理 5.68 知， G_1 实际上是 I_1 关于字典序 $x \prec z \prec y$ 的简化 Gröbner 基. 很清楚， I_1 关于 y 处于正规位置.

(2.4) 分解 G_1 中首项最低的成员，有 $y^6 - 3y^4 + 3y^2 - 1 = (y-1)^3(y+1)^3$.

(2.5),(2.6) 令 $E_2 = \mathrm{Id}(x - y^2 + 1, z - 1, y - 1)$, 且 $E_3 = \mathrm{Id}(x - y^2 + 1, z - 1, y + 1)$, 则获得如下两个确定的输出理想:

$$D_2 = E_2 : 1 = E_2 = \mathrm{Id}(x, y - 1, z - 1),$$
$$D_3 = E_3 : 1 = E_3 = \mathrm{Id}(x, y + 1, z - 1).$$

(3) 执行一次对 I_2 的如下化简:

对于字典序 $z \prec y \prec x$, 计算出 I_2 的简化 Gröbner 基 G_2 如下:

$$G_2 = \{x - y^2 - 1,\ y^6 + 3y^4 + 5y^2 + 3,\ z + 1\}.$$

注意到 $y^6 + 3y^4 + 5y^2 + 3$ 无实根，从而 $\sqrt[R]{I_2} = \mathrm{Id}(1)$.

由上面的定理，我们有 $\sqrt[R]{I} = D_1 \cap D_2 \cap D_3$. 注意到 $D_1 \subseteq D_i$, $i = 2, 3$. 于是, $\sqrt[R]{I} = D_1$, 即 $\sqrt[R]{I}$ 是 $\mathbb{Q}[x, y, z]$ 中由 $x - y^2 + z$ 和 $y^4 - 2zy^2 - z^3 + 2z^2$ 生成的实素理想.

§9.5 正定齐次多项式的有效表示

由 §4.2 中定义 4.2.1 知，序域上每个半正定多项式都可表示成若干个有理函数的平方和，只要这个域具有弱 Hilbert 性质. 作为一个相应的构造性问题，自然会问：是否存在一个有效的方法，使得 (具有弱 Hilbert 性质的) 可计算序域上每个半正定多项式都可表成若干个有理函数的平方和. 本节将考虑一种特殊情形：阿基米德序域上正定齐次多项式的平方和的有效表示. 本节的主要结果是由 W. Habicht[85] 首先获得的.

设 $(F,\leqslant)$ 是一个阿基米德序域. 根据定理 1.4.5, 可认定 $F\subseteq\mathbb{R}$, 且 $\leqslant$ 为 $\mathbb{R}$ 的惟一序在 F 上的限制. 因而，$(F,\leqslant)$ 上每个半正定多项式都可看作实数域 $\mathbb{R}$ 上的半正定多项式. F 上一个 n 元齐次多项式 f 称作在 $(F,\leqslant)$ 上是 (严格) 正定的，如果对于 F 中任意一组不全为零的元素 $a_1,\cdots,a_n$, $f(a_1,\cdots,a_n)>0$. F 上一个 n 元 d 次齐次多项式 f 称作是系数全为正的，如果它的所有 $\binom{n+d-1}{n-1}$ 项的系数都为 F 中正元素.

Habicht 的结果立足于 Pólya 所获得的一个结论 (参见文献 [148]). 因而，我们首先证明 Pólya 所获得的如下结论.

命题 9.5.1 设 $(F,\leqslant)$ 是一个阿基米德序域，$f:=f(x_1,\cdots,x_n)$ 是 F 上一个 n 元齐次多项式，使得对于 F 中任意一组元素 $a_1,\cdots,a_n$, $f(a_1,\cdots,a_n)>0$, 只要 $\sum\limits_{i=1}^{n}a_i>0$, 且 $a_i\geqslant0$, $i=1,\cdots,n$, 则存在某个充分大的自然数 r, 使得

$$(x_1+\cdots+x_n)^r f=g,$$

这里 g 是域 F 上一个系数全为正的齐次多项式.

证明 将 f 看作一个实多项式函数，且记

$$f=\sum_{j_1+\cdots+j_n=m}a_{j_1j_2\cdots j_n}\prod_{i=1}^{n}\frac{x_i^{j_i}}{j_i!},$$

其中 m 为 f 的次数，j_i 为非负整数，$i=1,\cdots,n$.

由条件知，f 在如下有界闭区域上是连续的且取正值：

$$D=\left\{(a_1,\cdots,a_n)\in\mathbb{R}^n\mid\sum_{i=1}^{n}a_i=1,\text{且}a_i\geqslant0,i=1\cdots,n\right\}.$$

从而，f 在 D 上有正的最小值 μ.

构造 F 上如下多项式：

$$\phi=\sum_{j_1+\cdots+j_n=m}a_{j_1j_2\cdots j_n}\prod_{i=1}^{n}\frac{x_i(x_i-t)\cdots(x_i-(j_i-1)t)}{j_i!}.$$

显然，$\phi \in F[x_1, \cdots, x_n, t] \subseteq \mathbb{R}[x_1, \cdots, x_n, t]$, 且 $\phi(x_1, \cdots, x_n, 0) = f$. 注意到，$\phi$ 在如下有界闭区域

$$D_1 = \left\{ (a_1, \cdots, a_n, b) \in \mathbb{R}^n \mid 0 \leqslant b \leqslant 1, \sum_{i=1}^{n} a_i = 1, \text{且} a_i \geqslant 0, i = 1 \cdots, n \right\}$$

上是一致连续的. 从而，有某个正元素 $\delta \in F$, 使得只要 $0 \leqslant b \leqslant \delta$, 且 $(a_1, \cdots, a_n) \in D$, 恒有

$$\phi(a_1, \cdots, a_n, b) > \phi(a_1, \cdots, a_n, 0) - \frac{1}{2}\mu = f(a_1, \cdots, a_n) - \frac{1}{2}\mu \geqslant \frac{1}{2}\mu > 0.$$

同时，对于每个大于 m 的自然数 r, 我们有

$$(x_1 + x_2 + \cdots + x_n)^{r-m} = (r-m)! \sum_{k_1+\cdots+k_n=r-m} \prod_{i=1}^{n} \frac{x_i^{k_i}}{k_i!},$$

其中 $k_i \geqslant 0$, $i = 1, \cdots, n$.

由此有

$$\begin{aligned}
&(x_1 + x_2 + \cdots + x_n)^{r-m} f \\
= \ & (r-m)! \sum_{j_1+\cdots+j_n=m} \sum_{k_1+\cdots+k_n=r-m} a_{j_1 j_2 \cdots j_n} \prod_{i=1}^{n} \frac{x_i^{j_i+k_i}}{j_i! k_i!},
\end{aligned}$$

令 $s_i = j_i + k_i$, $i = 1, \cdots, n$, 则有

$$\begin{aligned}
&(x_1 + x_2 + \cdots + x_n)^{r-m} f \\
= \ & (r-m)! \sum_{s_1+\cdots+s_n=r} \Big(\sum_{j_1+\cdots+j_n=m} \binom{s_1}{j_1} \cdots \binom{s_n}{j_n} a_{j_1 j_2 \cdots j_n} \Big) \prod_{i=1}^{n} \frac{x_i^{s_i}}{s_i!} \\
= \ & (r-m)! r^m \sum_{s_1+\cdots+s_n=r} \phi\left(\frac{s_1}{r}, \cdots, \frac{s_n}{r}, \frac{1}{r}\right) \prod_{i=1}^{n} \frac{x_i^{s_i}}{s_i!}.
\end{aligned}$$

由上面的讨论知，当 $\frac{1}{r} < \delta$, 即 $r > \frac{1}{\delta}$ 时，$\phi\left(\frac{s_1}{r}, \cdots, \frac{s_n}{r}, \frac{1}{r}\right) > 0$, 其中 $(s_1, \cdots, s_n)$ 取遍所有满足 $\sum_{i=1}^{n} s_i = r$ 的非负整数组. 证毕.

根据上面的命题，有理由给出如下定义.

定义 9.5.1 所设同命题 9.5.1. 使得齐次多项式 $(x_1 + \cdots + x_n)^r f$ 的系数全为正的最小指数 r 称作 f 的 Pólya 指数 .

由命题 9.5.1 及其证明可知，在命题 9.5.1 的所设条件下，$(x_1 + \cdots + x_n)^r f$ 是

域 F 上一个系数全为正的齐次多项式，只要 r 不小于 f 的 Pólya 指数. 然而，命题 9.5.1 只表明这样的自然数 r 的存在性，并未给出寻求它的一个有效算法. 为寻找这样一个有效算法， J. A. de Loera 和 F. Santos 进行了如下讨论.

设 $(F,\leqslant)$ 是一个阿基米德序域， $f := f(x_1,\cdots,x_n)$ 是 F 上一个次数为 d 的 n 元齐次多项式，使得对于 F 中任意一组不全为零的非负元素 $a_1,\cdots,a_n$, $f(a_1,\cdots,a_n) > 0$. 显然， f 可表为 $f = f^+ - f^-$, 其中 f^+ 和 f^- 都是 F 上具有非负系数的齐次多项式. 此时，令 $f_0 := f^+(x_1,\cdots,x_n) - f^-(x_1+d,\cdots,x_n+d)$, 则 $f_0 \in F[x_1,\cdots,x_n]$.

引理 9.5.2 所设同上，则

(1) $\Delta := \{(y_1,\cdots,y_n) \in \mathbb{R}^n \mid y_i \geqslant 0,\ i=1,\cdots,n,\ 且f_0(y_1,\cdots,y_n) \leqslant 0\}$ 是有界闭区域;

(2) 若 m 为 $\sum\limits_{i=1}^{n} x_i$ 在区域 Δ 上的最大值，则对于任意不小于 $m+dn$ 的自然数 r, $(x_1+\cdots+x_n)^r f$ 是域 F 上一个系数全为正的齐次多项式.

证明 显然， f_0 的最高次部分即为 f, 而其他低次项的系数均为负. 用 D 记作如下有界闭区域:

$$D = \left\{(a_1,\cdots,a_n) \in \mathbb{R}^n \mid \sum_{i=1}^{n} a_i = 1,\ 且a_i \geqslant 0,\ i=1\cdots,n\right\}.$$

于是，对于每个 $\alpha = (a_1,\cdots,a_n) \in D$, 单元多项式 $h_\alpha(x) := f_0(a_1x,\cdots,a_nx)$ 的首项系数为正，而其他项的系数为负. 由中间值定理和 Descartes 引理 (即命题 2.4.7) 知， $h_\alpha(x)$ 有惟一的正根. 记 $h_\alpha(x)$ 的惟一正根为 $\eta(\alpha)$, 则得 D 到 $\mathbb{R}$ 的一个映射 η, 使得对于每个 $\alpha \in D$, $\alpha \longmapsto \eta(\alpha)$. 易知， η 是一个连续映射. 由于 D 是 $\mathbb{R}$ 的一个有界闭区域，从而 η 在 D 上可达到最大值 e. 现设 $\beta = (a_1,\cdots,a_n) \in \Delta$ 且 $b := \sum\limits_{i=1}^{n} a_i$ 不为零，则 $\alpha := \left(\dfrac{a_1}{b},\cdots,\dfrac{a_n}{b}\right) \in D$. 当 $f_0(\beta) = 0$ 即 $h_\alpha(b) = 0$ 时，显然有 $b \leqslant e$. 当 $f_0(\beta) < 0$ 即 $h_\alpha(b) < 0$ 时，由于 $h_\alpha(x)$ 的首项系数为正，从而 $h_\alpha(x)$ 有一个根 c, 使得 $b < c$. 此时， $b < c \leqslant e$. 因而，叙述 (1) 获证.

再记

$$f = \sum_{j_1+\cdots+j_n=d} a_{j_1j_2\cdots j_n} \prod_{i=1}^{n} x_i^{j_i},$$

且

$$(x_1+\cdots+x_n)^r f = \sum_{k_1+\cdots+k_n=d+r} b_{k_1k_2\cdots k_n} \prod_{i=1}^{n} x_i^{k_i},$$

则系数 $b_{k_1k_2\cdots k_n}=\displaystyle\sum_{j_1+\cdots+j_n=d}\frac{r!}{(k_1-j_1)!\cdots(k_n-j_n)!}a_{j_1j_2\cdots j_n}$.

若 $k_i>d$, $i=1,\cdots,n$, 则可得如下不等式:

$$\begin{aligned}\frac{r!}{k_1!\cdots k_n!}k_1^{j_1}\cdots k_n^{j_n}&\geqslant\frac{r!}{(k_1-j_1)!\cdots(k_n-j_n)!}\\&\geqslant\frac{r!}{k_1!\cdots k_n!}(k_1-d)^{j_1}\cdots(k_n-d)^{j_n}.\end{aligned}$$

由此有

$$\begin{aligned}\frac{k_1!\cdots k_n!}{r!}b_{k_1k_2\cdots k_n}&\geqslant f^+(k_1-d,\cdots,k_n-d)-f^-(k_1,\cdots,k_n)\\&=f_0(k_1-d,\cdots,k_n-d).\end{aligned}$$

若 $k_1,\cdots,k_n$ 中有不大于 d 的数, 则不妨设 $k_1,\cdots,k_s>d\geqslant k_{s+1},\cdots,k_n$. 此时可得如下不等式:

$$\begin{aligned}&\frac{r!}{k_1!\cdots k_n!}k_1^{j_1}\cdots k_s^{j_s}d^{j_{s+1}}\cdots d^{j_n}\\\geqslant\ &\frac{r!}{(k_1-j_1)!\cdots(k_n-j_n)!}\\\geqslant\ &\frac{r!}{k_1!\cdots k_n!}(k_1-d)^{j_1}\cdots(k_s-d)^{j_s}0^{j_{s+1}+\cdots+j_n}.\end{aligned}$$

这里约定: $0^{j_{s+1}+\cdots+j_n}=0$ 或 1, 根据 $j_{s+1}+\cdots+j_n$ 为正或为零而定. 由此有

$$\begin{aligned}&\frac{k_1!\cdots k_n!}{r!}b_{k_1k_2\cdots k_n}\\\geqslant\ &f^+(k_1-d,\cdots,k_s-d,0,\cdots,0)-f^-(k_1,\cdots,k_s,d,\cdots,d)\\=\ &f_0(k_1-d,\cdots,k_s-d,0,\cdots,0).\end{aligned}$$

故总有 $(a_1,\cdots,a_n)\in\mathbb{R}^n$, 使得 $\displaystyle\sum_{i=1}^n a_i>r-dn$, 且 $\dfrac{k_1!\cdots k_n!}{r!}b_{k_1k_2\cdots k_n}\geqslant f_0(a_1,\cdots,a_n)$. 由自然数 r 的假定知, $(a_1,\cdots,a_n)\notin\Delta$, 即有 $f_0(a_1,\cdots,a_n)>0$. 因此, 全部系数 $b_{k_1k_2\cdots k_n}$ 都为正. 证毕.

定理 9.5.3 设 $(F,\leqslant)$ 是一个阿基米德序域, $f:=f(x_1,\cdots,x_n)$ 是 F 上一个次数为 d 的 n 元齐次多项式, 使得对于 F 中任意一组不全为零的非负元素 $a_1,\cdots,a_n$, $f(a_1,\cdots,a_n)>0$. 若 ℓ 是一个大于 2 以及 f 中所有系数的绝对值的数, 且 μ 是 f 在如下有界闭区域上的最小值:

$$D=\left\{(a_1,\cdots,a_n)\in\mathbb{R}^n \mid \sum_{i=1}^n a_i=1,\ 且a_i\geqslant 0,\ i=1\cdots,n\right\},$$

则对于任意大于 $\dfrac{2n\ell d^2}{\mu}+dn$ 的自然数 r, $(x_1+\cdots+x_n)^r f$ 是域 F 上一个系数全为正的齐次多项式.

证明 由引理 9.5.2 知, 仅需证明 $\dfrac{2n\ell d^2}{\mu}$ 是 $\sum\limits_{i=1}^n x_i$ 在区域 Δ 上的一个上界.

将区域 Δ 分成如下两部分:

$$\Delta_1:=\Delta\cap\left\{(y_1,\cdots,y_n)\in\mathbb{R}^n \mid \sum_{i=1}^n y_i\geqslant nd(d-1)\right\};$$

$$\Delta_2:=\Delta\cap\left\{(y_1,\cdots,y_n)\in\mathbb{R}^n \mid \sum_{i=1}^n y_i< nd(d-1)\right\}.$$

显然, $nd(d-1)$ 是 $\sum\limits_{i=1}^n x_i$ 在区域 Δ_2 上的一个上界. 由于 $\mu\leqslant f(1,0,\cdots,0)\leqslant \ell$, 从而 $nd(d-1)<2nd^2\leqslant\dfrac{2n\ell d^2}{\mu}$.

显然, 不等式 $f_0\leqslant 0$ 等价于

$$1\leqslant\frac{f^-(x_1+d,\cdots,x_n+d)-f^-}{f^+-f^-}=\frac{f^-(x_1+d,\cdots,x_n+d)-f^-}{f}.$$

因而有

$$\begin{aligned}\Delta_1:=\Bigg\{&(y_1,\cdots,y_n)\in\mathbb{R}^n \mid nd(d-1)\leqslant\sum_{i=1}^n y_i\\ &\leqslant\frac{(\sum_{i=1}^n y_i)\big(f^-(y_1+d,\cdots,y_n+d)-f^-(y_1,\cdots,y_n)\big)}{f(y_1,\cdots,y_n)},\\ &且\,y_i\geqslant 0,\ i=1,\cdots,n\Bigg\}.\end{aligned}$$

注意到, $\ell(\sum\limits_{i=1}^n x_i)^d-f^-$ 是一个具有非负系数的齐次多项式. 从而, 当 $x_i\geqslant 0$ $(i=1,\cdots,n)$ 时, $\ell(\sum\limits_{i=1}^n x_i)^d-f^-$ 对于每个变量都是递增的. 于是, 当 $x_i\geqslant 0$ $(i=1,\cdots,n)$ 时,

$$f^-(x_1+d,\cdots,x_n+d)-f^-\leqslant\ell(\sum_{i=1}^n x_i+nd)^d-\ell(\sum_{i=1}^n x_i)^d.$$

因而，对于每个 $(y_1,\cdots,y_n)\in\Delta_1$, 我们有

$$\sum_{i=1}^n y_i \leqslant \frac{\ell(\sum_{i=1}^n y_i)((\sum_{i=1}^n y_i+nd)^d-(\sum_{i=1}^n y_i)^d)}{f(y_1,\cdots,y_n)}.$$

对于 $(y_1,\cdots,y_n)\in\Delta_1$, 令 $b=\sum_{i=1}^n y_i$, 且 $\Psi(x)=\dfrac{x(bx+nd)^d-x(bx)^d}{x^d}$. 注意到，$\Psi(x)$ 的分子是一个系数均为正且次数为 d 的多项式. 因而，$\Psi(x)$ 在开区间 $]0,1[$ 上是递减的. 从而，$\Psi(1)\leqslant\Psi\left(\dfrac{nd(d-1)}{b}\right)$, 即 $(b+nd)^d-b^d\leqslant nd(d-1)b^{d-1}\left(\left(1+\dfrac{1}{d-1}\right)^d-1\right)$.

此外，由 μ 的规定知，$f(y_1,\cdots,y_n)=b^df(b^{-1}y_1,\cdots,b^{-1}y_n)\geqslant b^d\mu$. 根据上面的不等式，于是有

$$\begin{aligned}\sum_{i=1}^n y_i &\leqslant \frac{\ell nd(d-1)b^d\left((1+\frac{1}{d-1})^d-1\right)}{b^d\mu}\\ &=\frac{n\ell d(d-1)}{\mu}\left((1+\frac{1}{d-1})^d-1\right)\\ &=\frac{n\ell d^2}{\mu}\left((1+\frac{1}{d-1})^{d-1}-\frac{d-1}{d}\right).\end{aligned}$$

易知，当 $d\geqslant 4$ 时，$\left((1+\dfrac{1}{d-1})^{d-1}-\dfrac{d-1}{d}\right)<2.718\cdots-\dfrac{3}{4}=1.968\cdots$. 因而，对于大于 1 的自然数 d, $\left((1+\dfrac{1}{d-1})^{d-1}-\dfrac{d-1}{d}\right)<2$. 从而，定理获证.

现在，我们可以建立 Habicht 的如下结论.

定理 9.5.4 设 $(F,\leqslant)$ 是一个可计算的阿基米德序域，$f:=f(x_1,\cdots,x_n)$ 是 F 上一个正定的 n 元齐次多项式，则可有效地把 f 表示为如下形式：

$$f=\frac{\sum_{j=1}^r a_jg_j^2}{\sum_{k=1}^s b_kh_k^2},$$

其中 a_k 和 b_k 为 F 中正元素，g_j 和 h_k 是 F 上的齐次多项式，$j=1,\cdots,r;k=1,\cdots,s$.

证明 设 f 的次数为 $2d$. 我们的计算过程分成如下步骤：

(1) 引进辅助变量 z, 而考虑 $n+1$ 元齐次式 $\phi(x_1,\cdots,x_n,z):=z^{2d}+f$. 显然，

ϕ 在 F 上也是正定的. 记 $\Lambda := \{\lambda = (\lambda_1, \cdots, \lambda_{n+1}) \mid \lambda_i = 1或-1, i = 1, \cdots, n+1\}$, 且构造 F 上如下齐次式:

$$\Phi = \prod_{\lambda \in \Lambda} \phi(\lambda_1 x_1, \cdots, \lambda_n x_n, \lambda_{n+1} z).$$

(2) 通过展开可将 Φ 表为: $\Phi = \Psi(x_1^2, \cdots, x_n^2, z^2)$, 其中 $\Psi \in F[x_1, \cdots, x_n, z]$. 显然, 齐次式 Ψ 满足定理 9.5.3 中的条件. 根据定理 9.5.3, 可计算出一个自然数 r, 使得 $(x_1 + \cdots + x_n + z)^r \Psi$ 的全部系数均为正. 记 e 为齐次式 $(x_1 + \cdots + x_n + z)^r \Psi$ 的次数, 则有

$$(x_1^2 + \cdots + x_n^2 + z^2)^r \Phi = \sum_{i+j_1+\cdots+j_n=e} c_{ij_1\cdots j_n} (x_1^{j_1} \cdots x_n^{j_n} z^i)^2,$$

其中所有的系数 $c_{ij_1\cdots j_n}$ 均为 F 中正元素.

注意到, ϕ 是多项式 $(x_1^2 + \cdots + x_n^2 + z^2)^r \Phi$ 的一个因式. 于是有齐次式 $\eta \in F[x_1, \cdots, x_n, z]$, 使得如下等式成立:

$$\eta\phi = \sum_{i+j_1+\cdots+j_n=e} c_{ij_1\cdots j_n} (x_1^{j_1} \cdots x_n^{j_n} z^i)^2.$$

通过整数的带余除法有, $i = 2dq_i + k_i$, 其中 q_i 和 k_i 均为非负整数, 且 $0 \leqslant k_i \leqslant 2d-1$. 从而 $z^i = [(z^{2d})^{q_i} - (-f)^{q_i}] z^{k_i} + (-f)^{q_i} z^{k_i}$. 注意到, $(z^{2d})^{q_i} - (-f)^{q_i}$ 可被 ϕ 整除. 于是有

$$x_1^{j_1} \cdots x_n^{j_n} z^i = \phi u_{ij_1\cdots j_n} + w_{ij_1\cdots j_n} z^{k_i},$$

其中 $w_{ij_1\cdots j_n} = x_1^{j_1} \cdots x_n^{j_n} (-f)^{q_i}$, 而 $u_{ij_1\cdots j_n}$ 为 $F[x_1, \cdots, x_n, z]$ 中齐次式.

把这些关系代入前面等式的右端, 并将可被 ϕ 整除的部分移往左端, 则得

$$\xi\phi = \sum_{k=0}^{2d-1} \left(\sum_{\substack{i+j_1+\cdots+j_n=e \\ 2d|i-k}} c_{ij_1\cdots j_n} w_{ij_1\cdots j_n}^2 \right) z^{2k}.$$

其中 ξ 是 $F[x_1, \cdots, x_n, z]$ 中一个齐次式.

将 ϕ 和 ξ 都看作 $F[x_1, \cdots, x_n]$ 上含 z 的单元多项式, 则 ξ 中 z 的最高指数不超过 $2d-2$. 记 g 为 ξ 中零次项 z^0 的系数, 且比较上式两端中 z^0 和 z^{2d} 的系数, 则有

$$fg = \sum_{\substack{i+j_1+\cdots+j_n=e \\ 2d|i}} c_{ij_1\cdots j_n} w_{ij_1\cdots j_n}^2, \text{ 且 } g = \sum_{\substack{i+j_1+\cdots+j_n=e \\ 2d|i-d}} c_{ij_1\cdots j_n} w_{ij_1\cdots j_n}^2.$$

由此可将 f 表为所求的形式. 证毕.

应该注意，本节的方法不适用于非阿基米德序域的情形．其原因是因为命题 9.5.1 对于非阿基米德序域不成立，见下例．

例 设 $F=\mathbb{Q}(\epsilon)$, 其中 ϵ 是有理数域 $\mathbb{Q}$ 上的一个未定元．根据定理 2.6.4 知，域 F 有一个序 $\leqslant$, 使得 ϵ 在 $\mathbb{Q}$ 上是正的无限小元素．令 $f(x,y)=(x-y)^2+\epsilon xy$, 则 $f(x,y)$ 是 F 上一个二元齐次式．显然，对于 $a,b\in F$, 总有 $f(a,b)>0$, 只要 $a\geqslant 0$, $b\geqslant 0$, 且 $a+b>0$. 然而，可断言：对于每个自然数 r, 齐次式 $(x+y)^r f(x,y)$ 中都有系数为负的项．

事实上，$(x+y)f(x,y)$ 中项 xy^2 的系数为负元素 $\epsilon-1$; 当 $r=2k$ 为偶数时，项 $x^{k+1}y^{k+1}$ 的系数为 $2\binom{2k}{k-1}-(2-\epsilon)\binom{2k}{k}=\binom{2k}{k}\epsilon-\dfrac{2(2k)!}{(k-1)!k!}\left(\dfrac{1}{k}-\dfrac{1}{k+1}\right)<0$; 当 $r=2k+1$ 为大于 1 的奇数时，项 $x^{k+1}y^{k+2}$ 的系数为 $\binom{2k+1}{k-1}+\binom{2k+1}{k+1}-(2-\epsilon)\binom{2k+1}{k}=\binom{2k+1}{k}\epsilon-\dfrac{(2k+1)!}{(k-1)!(k+1)!}\left(\dfrac{1}{k}-\dfrac{1}{k+2}\right)<0$.

§9.6 柱形代数分解

柱形代数分解是 G. E. Collins 在 20 世纪 70 年代中提出的一个有效方法，它适用于实闭域的量词消去．这一方法在实用方面具有比 Tarski-Seidenberg 原理更高的效率．因此，柱形代数分解可作为工具来处理一些实际问题．

在介绍柱形代数分解之前，我们需要一些预备知识．设 F 是一个域．给定域 F 上如下两个非零多项式：

$$f(x)=a_0x^m+a_1x^{m-1}+\cdots+a_m,$$
$$g(x)=b_0x^n+b_1x^{n-1}+\cdots+b_n,$$

其中 a_0 和 b_0 不全为零．

对于 $i=0,\cdots,\min\{m,n\}$, 规定 F 上如下 $(m+n-2i)\times(m+n-i)$ 矩阵：

$$M_i=\begin{pmatrix} a_0 & a_1 & \cdots & a_m & & & \\ & a_0 & a_1 & \cdots & a_m & & \\ & & \vdots & \vdots & \vdots & & \\ & & a_0 & a_1 & \cdots & a_m & \\ b_0 & b_1 & \cdots & b_n & & & \\ & b_0 & b_1 & \cdots & b_n & & \\ & & \vdots & \vdots & \vdots & & \\ & & b_0 & b_1 & \cdots & b_n & \end{pmatrix}\begin{matrix} \left.\begin{matrix}\\ \\ \\ \\ \end{matrix}\right\} n-i\text{行} \\ \left.\begin{matrix}\\ \\ \\ \\ \end{matrix}\right\} m-i\text{行}\end{matrix}$$

进一步，用 M_{i0} 表示矩阵 M_i 中前 $m+n-2i$ 列所组成的子矩阵．此外，用

$\mathrm{Psc}_i(f,g;x)$ 表示矩阵 M_{i0} 的行列式，且称 $\mathrm{Psc}_i(f,g;x)$ 为 $f(x)$ 和 $g(x)$ 关于 x 的第 i 个主子结式系数.

命题 9.6.1 设 $f(x)$, $g(x)$ 同上，则 $f(x)$ 和 $g(x)$ 的最大公因式的次数为 k, 当且仅当 $\mathrm{Psc}_0(f,g;x)=\mathrm{Psc}_1(f,g;x)=\cdots=\mathrm{Psc}_{k-1}(f,g;x)=0$, 但 $\mathrm{Psc}_k(f,g;x)\neq 0$.

证明 由矩阵 M_i 的规定，显然有

$$M_i\begin{pmatrix} x^{m+n-i-1} \\ x^{m+n-i-2} \\ \vdots \\ x \\ 1 \end{pmatrix}=\begin{pmatrix} x^{n-i-1}f(x) \\ \vdots \\ f(x) \\ x^{m-i-1}g(x) \\ \vdots \\ g(x) \end{pmatrix}.$$

设 $d(x)$ 是 $f(x)$ 和 $g(x)$ 的一个最大公因式，则 $\dfrac{g(x)}{d(x)}f(x)-\dfrac{f(x)}{d(x)}g(x)=0$. 若 $d(x)$ 的次数为 k, 则 $\dfrac{g(x)}{d(x)}$ 的次数不超过 $n-k$, 而 $\dfrac{f(x)}{d(x)}$ 的次数不超过 $m-k$. 当 $i=0,\ 1,\ \cdots,\ k-1$ 时，由等式 $\dfrac{g(x)}{d(x)}f(x)-\dfrac{f(x)}{d(x)}g(x)=0$ 知，有不全为零的元素 $c_1,\cdots,c_{m+n-2i}\in F$, 使得

$$(c_1,\cdots,c_{m+n-2i})\begin{pmatrix} x^{n-i-1}f(x) \\ \vdots \\ f(x) \\ x^{m-i-1}g(x) \\ \vdots \\ g(x) \end{pmatrix}=0,$$

即

$$(c_1,\cdots,c_{m+n-2i})M_i\begin{pmatrix} x^{m+n-i-1} \\ x^{m+n-i-2} \\ \vdots \\ x \\ 1 \end{pmatrix}=0.$$

从而有 $(c_1,\cdots,c_{m+n-2i})M_i=0$.

这表明矩阵 M_i 的秩小于 $m+n-2i$, 从而 $\mathrm{Psc}_i(f,g;x)$ 作为 M_i 的一个 $m+n-2i$

级子式必有零.

假若 $\mathrm{Psc}_k(f,g;x)=0$, 则矩阵 M_{k0} 的秩小于 $m+n-2k$. 从而有不全为零的 $c_1,\cdots,c_{m+n-2k}\in F$, 使得

$$(c_1,\cdots,c_{m+n-2k})M_{k0}=0.$$

显然, 矩阵 M_k 可分块为 $M_k=(M_{k0},M^{\mathrm{T}})$, 这里 M^{T} 是 F 上一个 $(m+n-2k)\times k$ 矩阵.

构造域 F 上的如下多项式:

$$w(x)=(c_1,\cdots,c_{m+n-2k})M_k\begin{pmatrix}x^{m+n-k-1}\\x^{m+n-k-2}\\\vdots\\x\\1\end{pmatrix},$$

则

$$w(x)=(c_1,\cdots,c_{m+n-2k})M^{\mathrm{T}}\begin{pmatrix}x^{k-1}\\\vdots\\x\\1\end{pmatrix}.$$

从而 $w(x)$ 的次数不超过 $k-1$. 另一方面，由上面的矩阵等式知,

$$w(x)=(c_1,\cdots,c_{m+n-2k})\begin{pmatrix}x^{n-k-1}f(x)\\\vdots\\f(x)\\x^{m-k-1}g(x)\\\vdots\\g(x)\end{pmatrix}=u(x)f(x)+v(x)g(x).$$

其中 $u(x)$ 和 $v(x)$ 是 F 上不全为零的多项式，$u(x)$ 的次数不超过 $n-k-1$, 而 $v(x)$ 的次数不超过 $m-k-1$.

此时, 显然 $d(x)$ 整除 $w(x)$. 由于 $d(x)$ 的次数超过 $w(x)$ 的次数, 从而 $w(x)=0$, 由此有 $u(x)f(x)=-v(x)g(x)$. 从而可知，$u(x)$ 和 $v(x)$ 都是非零多项式. 由条件, 不妨设 $a_0\neq 0$. 注意到 $u(x)\dfrac{f(x)}{d(x)}=-v(x)\dfrac{g(x)}{d(x)}$, 且 $\dfrac{f(x)}{d(x)}$ 与 $\dfrac{g(x)}{d(x)}$ 互素，从而 $\dfrac{f(x)}{d(x)}$

整除 $v(x)$; 这是不可能, 因为 $\frac{f(x)}{d(x)}$ 的次数大于 $v(x)$ 的次数. 因而 $\mathrm{Psc}_k(f,g;x)\neq 0$. 从而, 命题的必要性获证.

现设 $\mathrm{Psc}_i(f,g;x)=0$, $i=0,1,\cdots,k-1$, 但 $\mathrm{Psc}_k(f,g;x)\neq 0$. 又设 $f(x)$ 和 $g(x)$ 的最大公因式的次数为 k'. 由必要性的证明知, $\mathrm{Psc}_0(f,g;x)=\mathrm{Psc}_1(f,g;x)=\cdots=\mathrm{Psc}_{k'-1}(f,g;x)=0$, 但 $\mathrm{Psc}_k(f,g;x)\neq 0$. 从而必有 $k'=k$. 因而, 充分性成立. 证毕.

设 $(F,\leqslant)$ 是一个序域, R 是 F 的一个实闭扩张, 使得 R 的惟一序是 F 的序 $\leqslant$ 的一个拓展, 且 R 的惟一序也记作: $\leqslant$. 对于 $n\in\mathbb{N}$, 用 R^n 表示 R 上的 n 维仿射空间. 由 §1.2 知, R 关于序 $\leqslant$ 的区间拓扑诱导出 R^n 的一个所谓的乘积区间拓扑, 使得 R^n 成为一个 Hausdorff 拓扑空间. R^n 的一个半代数子集 S 称作是半代数连通的, 如果 S 不能表为两个不相交的非空半代数子集 S_1 和 S_2 的并, 使得 S_1 和 S_2 在 S 中都是闭的. 根据文献 [25] 中命题 2.4.3, R^n 中开的超立方体 $]0,1[^n$ 是半代数连通的. 因此, 每个半代数同胚于 $]0,1[^n$ 的半代数子集都是半代数连通的.

设 S 是 R^n 的一个非空子集. 对于 S 到 R 的一个映射 ψ, 称: 在 S 上恒有 $\psi<0$, 如果对于所有 $\alpha\in S$, 恒有 $\psi(\alpha)<0$. 在完全类似的意义下, 我们可称: 在 S 上恒有 $\psi=0$, $\psi\neq 0$, $\psi>0$ 或 $\psi\leqslant 0$ 等等. 在如此任一情况下, 统称 ψ 在 S 上是不变的. 对于域 F 上每个 n 元多项式 f, f 可看作 S 到 R 的一个映射, 从而叙述 "f 在 S 上是不变的" 有明确的意义. 对于由域 F 上 n 元多项式组成的一个非空集 A, 称 A 在 S 上是不变的, 如果 A 中每个多项式在 S 上是不变的.

设 $F[x_1,\cdots,x_n]$ 是域 F 上 n 元多项式环. 对于每个非零多项式 $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$, $f(x_1,\cdots,x_n)$ 可表为

$$f(x_1,\cdots,x_n)=h_m x_n^m+h_{m-1}x_n^{m-1}+\cdots+h_0,$$

其中 $h_i\in F[x_1,\cdots,x_{n-1}]$, $i=0,1,\cdots,m$, 且 $h_m\neq 0$. 此时, 称 m 为 f 关于变量 x_n 的次数, $h_m x_n^m$ 为 f 关于 x_n 的首项, h_m 为 f 关于 x_n 的首项系数, 且它们分别用 $\deg(f;x_n)$, $\mathrm{ldt}(f;x_n)$, $\mathrm{ldc}(f;x_n)$ 表示. 而且, 称多项式 $f-\mathrm{ldt}(f;x_n)$ 为 f 关于 x_n 的缩简, 且记之为 $\mathrm{red}(f;x_n)$. 为方便起见, 约定: $\mathrm{ldt}(0;x_n)=\mathrm{ldc}(0;x_n)=\mathrm{red}(0;x_n)=0$, 而 $\deg(0;x_n)=-\infty$.

借助于归纳定义, 对于上述的非零多项式 f 以及非负整数 k, 规定

$$\mathrm{red}^0(f;x_n)=f,\ \text{且}\ \mathrm{red}^{k+1}(f;x_n)=\mathrm{red}\big(\mathrm{red}^k(f;x_n);x_n\big).$$

此时, 称 $\mathrm{red}^k(f;x_n)$ 为 f 关于 x_n 的第 k 次缩简, 其中 $k\geqslant 0$. 显然, $\mathrm{red}^k(f;x_n)=0$, 只要 $k>\deg(f;x_n)+1$.

定义 9.6.1 设 S 是 R^{n-1} 的一个子集. 对于 $F[x_1,\cdots,x_n]$ 中一个非零多项式

f, 称 f 的根在 S 上是可描绘的，如果存在 S 到 R 中的连续半代数映射 $\psi_1, \cdots, \psi_k, k \geqslant 0$, 使得下列条件成立:

(1) 存在自然数 $e_1, \cdots, e_m, m \geqslant k$, 使得对于每个 $(a_1, \cdots, a_{n-1}) \in S$, $f(a_1, \cdots, a_{n-1}, x)$ 恰有 m 个相异的根，且这些根的重数分别为 $e_1, \cdots, e_m$;

(2) 对于每个 $(a_1, \cdots, a_{n-1}) \in S$, $\psi_1(a_1, \cdots, a_{n-1}) < \cdots < \psi_k(a_1, \cdots, a_{n-1})$;

(3) 对于每个 $(a_1, \cdots, a_{n-1}) \in S$, $\psi_i(a_1, \cdots, a_{n-1})$ 是 $f(a_1, \cdots, a_{n-1}, x)$ 的一个重数为 e_i 的根, $i = 1, \cdots, k$;

(4) 若 $f(a_1, \cdots, a_{n-1}, b) = 0$, 其中 $(a_1, \cdots, a_{n-1}) \in S$ 且 $b \in R$, 则对于某个 $j \in \{1, \cdots, k\}$, $b = \psi_j(a_1, \cdots, a_{n-1})$.

此时，我们称 $\psi_1, \cdots, \psi_k$ 在 S 上描绘 f 在 R 中的根，且称 e_i 为 ψ_i 的重数, $i = 1, \cdots, k$.

更一般地，设 $f_1, \cdots, f_s$ 是 $F[x_1, \cdots, x_n]$ 中有限个多项式，且 $f_1, \cdots, f_r$ 在 S 上不恒为零，但 $f_{r+1}, \cdots, f_s$ 在 S 上都恒为零. 如果多项式积 $f_1 \cdots f_r$ 的根在 S 上是可描绘的，则称 $\{f_1, \cdots, f_s\}$ 的根在 S 上是可描绘的.

定理 9.6.2 设 $f \in F[x_1, \cdots, x_n]$, 且 S 是 R^{n-1} 的一个半代数连通子集. 如果在 S 上，恒有 $\mathrm{ldc}(f; x_n) \neq 0$, 且 f 的相异根个数保持不变，则 f 的根在 S 上是可描绘的.

证明 可假定 $S \neq \emptyset$ 且 $\deg(f; x_n) > 0$. 由条件可设，f 在 S 上的相异根个数恒为 m. 对于 $i = 1, \cdots, m$. 可构造 S 的如下子集:

$$S_i = \{(a_1, \cdots, a_{n-1}) \in S \mid f(a_1, \cdots, a_{n-1}, x)\text{在}R\text{中恰有}i\text{个相异根}\}.$$

显然，$S = \bigcup_{i=1}^{m} S_i$, 且易知 S_i 是 R^{n-1} 的一个半代数子集, $i = 1, \cdots, m$.

设 $(a_1, \cdots, a_{n-1}) \in S_i$, 则 $f(a_1, \cdots, a_{n-1}, x)$ 在 R 中恰有 i 个相异根 $\alpha_1 < \cdots < \alpha_i$. 由条件知，$f(a_1, \cdots, a_{n-1}, x)$ 还有 $m - i$ 个相异根属于 $R(\sqrt{-1})$ 但不属于 R, 这些根记作: $\alpha_{i+1}, \cdots, \alpha_m$. 记 e_j 为根 α_j 的重数, $j = 1, \cdots, m$. 当 $m = 1$ 时，令 $\delta = 1$; 否则，令 $\delta = \frac{1}{2}\min\{|\alpha_i - \alpha_j| \mid 1 \leqslant i < j \leqslant m\}$, 这里 $|\cdot|$ 表示 $R(\sqrt{-1})$ 上关于正锥 R^2 的绝对值. 作为 $F[x_1, \cdots, x_{n-1}]$ 上含未定元 x_n 的一个多项式，f 的全部系数都是在 S 上的连续函数，且 $\mathrm{ldc}(f; x_n)$ 在 S 上保持不为零. 根据引理 4.2.3 可知，存在 F 中一个正元素 ϵ, 使得对于任意 $(a'_1, \cdots, a'_{n-1}) \in S$, 只要 $|a'_r - a_r| < \epsilon, r = 1, \cdots, n-1$, 多项式 $f(a'_1, \cdots, a'_{n-1}, x)$ 在 $R(\sqrt{-1})$ 中恰有 e_j 个根 y, 满足 $|y - \alpha_j| < \delta$. 由条件知，$f(a'_1, \cdots, a'_{n-1}, x)$ 恰有 m 个相异根. 因此, $f(a'_1, \cdots, a'_{n-1}, x)$ 在 $R(\sqrt{-1})$ 中仅有一个相异根 y_j, 使得 $|y_j - \alpha_j| < \delta, j = 1, \cdots, m$. 这表明 y_j 的重数也为 $e_j, j = 1, \cdots, m$. 此时可断定: $y_j \in R, j = 1, \cdots, i$. 事实上，若对于某个 $j_0 \in \{1, \cdots, i\}$, $y_{j_0} \notin R$, 则 $f(a'_1, \cdots, a'_{n-1}, x)$ 在 $R(\sqrt{-1})$ 有另一

根 $\bar{y}_{j_0}$, 使得 $|\bar{y}_{j_0}-\alpha_{j_0}|<\delta$, 这里 $\bar{y}_{j_0}$ 为 y_{j_0} 在 R 上的共轭元, 矛盾. 又假若对于某个 $j_0\in\{i+1,\cdots,m\}$, $y_{j_0}\in R$, 则 $|y_{j_0}-\alpha_{j_0}|=|y_{j_0}-\bar{\alpha}_{j_0}|<\delta$. 由此有 $|\alpha_{j_0}-\bar{\alpha}_{j_0}|<2\delta$, 矛盾. 因而, $y_j\notin R$, $j=i+1,\cdots,m$. 于是由 S_i 的规定知, $(a_1',\cdots,a_{n-1}')\in S_i$, 只要 $(a_1',\cdots,a_{n-1}')\in S$ 且 $|a_r'-a_r|<\epsilon$, $r=1,\cdots,n-1$. 这表明 S_i 是 S 的一个开子集, $i=1,\cdots,m$.

由所设知, S 是半代数连通的. 从而, 对于某个 $k\in\{1,\cdots,m\}$, $S=S_k$. 因而, 对于每个 $(a_1,\cdots,a_{n-1})\in S$, $f(a_1,\cdots,a_{n-1},x)$ 在 R 中恰有 k 个相异根 $\alpha_1<\cdots<\alpha_k$. 据此, 对于 $j=1,\cdots,k$, 可作 S 到 R 的一个映射 ψ_j, 使得 $\psi_j(a_1,\cdots,a_{n-1})=\alpha_j$. 借助于引理 4.2.3 可知, ψ_j 是一个连续的半代数映射, $j=1,\cdots,k$. 由上面的讨论知, 在 S 上 $\psi_1,\cdots,\psi_k$ 描绘 f 在 R 中的根. 证毕.

现设 $A=\{f_1,\cdots,f_s\}\subset F[x_1,\cdots,x_n]$, 其中 $f_i\neq 0$, $i=1,\cdots,s$, 则可构造 $F[x_1,\cdots,x_n]$ 的如下子集:

$$B=\{\mathrm{red}^k(f;x_n)\mid f\in A,\ 0\leqslant k\leqslant \deg(f;x_n)\ \text{且}\ \mathrm{red}^k(f;x_n)\neq 0\}.$$

显然, $A\subseteq B$. 在此基础上, 可进一步构造 $F[x_1,\cdots,x_{n-1}]$ 的如下子集:

$$L=\{\mathrm{ldc}(g;x_n)\mid g\in B\};$$

$$E_1=\left\{\mathrm{Psc}_k\left(g,\frac{\partial g}{\partial x_n};x_n\right)\mid g\in B\ \text{且}\ 0\leqslant k\leqslant \deg\left(\frac{\partial g}{\partial x_n};x_n\right)\right\};$$

$$E_2=\{\mathrm{Psc}_k(g,h;x_n)\mid g,h\in B\ \text{且}\ 0\leqslant k\leqslant \min\{\deg(g;x_n),\deg(g;x_n)\}\}.$$

于是, 我们得到 $F[x_1,\cdots,x_n]$ 的一个有限子集 $L\cup E_1\cap E_2$. 所得的这样一个子集称作 A 关于 x_n 的投影, 且记作: $\mathrm{Proj}(A;x_n)$.

下面定理反映出上面所规定的投影 $\mathrm{Proj}(A;x_n)$ 的重要作用.

定理 9.6.3 设 A 同上, 且 S 是 R^{n-1} 的一个半代数连通子集. 如果 $\mathrm{Proj}(A;x_n)$ 在 S 上是不变的, 则 A 的根在 S 上是可描绘的, 且存在 S 到 R 的连续半代数映射 $\psi_1,\cdots,\psi_k$, 使得 $\psi_1,\cdots,\psi_k$ 在 S 上描绘 A 在 R 中的根, 且对于每个 $f\in A$, 在 S 上 f 在 R 中的根可通过 $\psi_1,\cdots,\psi_k$ 中某些映射来描绘.

证明 首先证明: 对于每个 $f\in A$, f 的根在 S 上是可描绘的.

设 $f=\sum\limits_{i=0}^{r}h_ix_n^i$. 显然, $h_i\in L$, 如果 $0\leqslant i\leqslant r$ 且 $h_i\neq 0$. 因此, h_i 在 S 上不变, $i=0,\cdots,r$. 若在 S 上 f 恒为零, 即 $h_i=0$, $i=1,\cdots,r$, 则上面的结论显然. 否则, 存在最大的指标 m, 使得在 S 上恒有 $h_m\neq 0$. 令 $g=\sum\limits_{i=0}^{m}h_ix_n^i$, 则对于某个非负整数 r, $g=\mathrm{red}^r(f)\in B$. 于是, $\mathrm{Psc}_j\left(g,\dfrac{\partial g}{\partial x_n};x_n\right)\in E_1$ 在 S 上是不变的, $j=0,\cdots,m-1$.

注意到,在 S 上恒有 $\mathrm{Psc}_{m-1}\left(g,\dfrac{\partial g}{\partial x_n};x_n\right)=mh_m\neq 0$. 从而存在非负整数 k, 使得在 S 上恒有 $\mathrm{Psc}_j\left(g,\dfrac{\partial g}{\partial x_n};x_n\right)=0, j=0,\cdots,k-1$, 但 $\mathrm{Psc}_k\left(g,\dfrac{\partial g}{\partial x_n};x_n\right)\neq 0$. 由命题 9.6.1 可知, 对于每个 $(a_1,\cdots,a_{n-1})\in S$, $g(a_1,\cdots,a_{n-1},x)$ 与 $\dfrac{\partial g}{\partial x_n}(a_1,\cdots,a_{n-1},x)$ 的最大公因式的次数恒为 k. 因而, $g(a_1,\cdots,a_{n-1},x)$ 的相异根的个数恒为 $m-k$. 由定理 9.6.2 知, g 的根在 S 上是可描绘的. 由于在 S 上恒有 $f=g$, 从而 f 的根在 S 上是可描绘的.

现在, 我们来证明定理中结论. 为此, 令 $A=\{f_1,\cdots,f_s\}$. 若 A 中每个多项式在 S 上恒为零, 则定理显然成立. 下设 $f_1,\cdots,f_r$ 在 S 上不恒为零, 而$f_{r+1},\cdots,f_s$ 在 S 上恒为零, 这里 $1\leqslant r\leqslant s$. 由上面讨论可见, 有 $g_i\in B$, 使得在 S 上, 恒有 $f_i=g_i$ 且 $\mathrm{ldc}(g_i;x_n)\neq 0$, $i=1,\cdots,r$. 当 $1\leqslant i<j\leqslant r$ 时, $\mathrm{Psc}_k(g_i,g_j;x_n)\in E_2\subseteq \mathrm{Proj}(A;x_n)$, 其中 $0\leqslant k\leqslant \min\{\deg(g_i;x_n),\deg(g_j;x_n)\}$. 类似于上面的讨论可知, g_i 和 g_j 的公共根个数在 S 上是不变的, 只要 $1\leqslant i<j\leqslant r$. 对于任意取定的 $(a_1,\cdots,a_{n-1})\in S$ 以及 $F[x_1,\cdots,x_n]$ 中两个非零多项式 u, v, 用 $\#(u)$ 表示 $u(a_1,..,a_{n-1},x)$ 的相异根个数, 而 $\#(u,v)$ 表示 $u(a_1,\cdots,a_{n-1},x)$ 和 $u(a_1,\cdots,a_{n-1},x)$ 的公共根个数. 此时, 如下递推关系式显然成立:

$$
\begin{aligned}
&(1)\#(g_1\cdots g_{k-1},g_k)\ =\#(g_1\cdots g_{k-2},g_k)+\#(g_{k-1},g_k)\\
&\qquad\qquad\qquad\qquad -\#(g_1\cdots g_{k-2},g_{k-1});\\
&(2)\#(g_1\cdots g_k)=\#(g_1\cdots g_{k-1})+\#(g_k)-\#(g_1\cdots g_{k-1},g_k).
\end{aligned}
$$

借助于上面递推关系, $\#(g_1\cdots g_k)$ 可通过 $\#(g_i)$ 和 $\#(g_i,g_j)$ 来表达, 这里 $1\leqslant i<j\leqslant r$. 由上面的讨论可见, $\#(g_i)$ 和 $\#(g_i,g_j)$ 在 S 上是不变的. 因此, $\#(g_1\cdots g_k)$ 在 S 上也是不变的. 由定理 6.9.2 知, $g_1\cdots g_r$ 的根在 S 上是可描绘. 从而 $f_1\cdots f_r$ 的根在 S 上是可描绘的.

设 $\psi_1<\cdots<\psi_k$ 是 S 到 R 的 k 个连续半代数映射, 且它们在 S 上描绘 $f_1\cdots f_r$ 在 R 中的根. 另一方面, 由首先证明的事实, 可设 f_i 在 R 中的根可通过连续半代数映射 $\phi_{i1}<\cdots<\phi_{ik_i}$ 在 S 上来描绘, $i=1,\cdots,r$. 记 $\phi_1,\cdots,\phi_\ell$ 是 $\{\phi_{ij_i}\mid 1\leqslant i\leqslant r\text{而}1\leqslant j_i\leqslant k_i\}$ 中全部相异的映射. 对于任意取定的 $(a_1,\cdots,a_{n-1})\in S$, $\psi_1(a_1,\cdots,a_{n-1})$ 是 $f_1(a_1,\cdots,a_{n-1},x)\cdots f_r(a_1,\cdots,a_{n-1},x)$ 在 R 中的一个根, 从而也是 $f_1(a_1,\cdots,a_{n-1},x),\cdots,f_r(a_1,\cdots,a_{n-1},x)$ 中某个多项式的根. 由定义 9.6.1 中条件 (4), 可设 $\psi_1(a_1,\cdots,a_{n-1})=\phi_1(a_1,\cdots,a_{n-1})$.

作 S 的如下两个子集:

$$
\begin{aligned}
S_1&=\{(y_1,\cdots,y_{n-1})\in S\mid \phi_1(y_1,\cdots,y_{n-1})\neq\psi_j(y_1,\cdots,y_{n-1}),\ j=2,\cdots,k\};\\
S_2&=\{(y_1,\cdots,y_{n-1})\in S\mid \phi_1(y_1,\cdots,y_{n-1})\neq\psi_1(y_1,\cdots,y_{n-1})\}.
\end{aligned}
$$

假若 $\psi_1 \neq \phi_1$, 则对于某个 $(b_1, \cdots, b_{n-1}) \in S$, 我们有

$$\phi_1(b_1, \cdots, b_{n-1}) \neq \psi_1(b_1, \cdots, b_{n-1}).$$

此时显然有, $(a_1, \cdots, a_{n-1}) \in S_1$, 但 $(b_1, \cdots, b_{n-1}) \in S_2$. 易知, S_1 和 S_2 是 S 的两个不相交的半代数开子集, 且 $S = S_1 \cup S_2$; 这矛盾于 S 的半代数连通性. 因而 $\psi_1 = \phi_1$. 重复这样的讨论可知, $\ell = k$, 且适当地调整下标后, 有 $\phi_i = \psi_i, i = 1, \cdots, k$. 至此定理证毕.

定义 9.6.2 设 S 是 R^{n-1} 的一个非空子集, $\psi_1, \cdots, \psi_k$ 都是 S 到 R 的连续映射, 且在 S 上恒有 $\psi_1 < \cdots < \psi_k$. 柱形 $S \times R$ 关于 $\psi_1, \cdots, \psi_k$ 的分解是指 $S \times R$ 的这样一个分块 $\{S_1, \cdots, S_{2k+1}\}$, 其中

$$S_1 = \{(\bar{\alpha}, a) \mid \bar{\alpha} \in S, \text{ 且} a < \psi_1(\bar{\alpha})\};$$
$$S_2 = \{(\bar{\alpha}, a) \mid \bar{\alpha} \in S, \text{ 且} a = \psi_1(\bar{\alpha})\};$$
$$\cdots\cdots$$
$$S_{2j-1} = \{(\bar{\alpha}, a) \mid \bar{\alpha} \in S, \text{ 且} \psi_{j-1}(\bar{\alpha}) < a < \psi_j(\bar{\alpha})\}; 2 \leqslant j \leqslant k$$
$$S_{2j} = \{(\bar{\alpha}, a) \mid \bar{\alpha} \in S, \text{ 且} a = \psi_j(\bar{\alpha})\}; 2 \leqslant j \leqslant k$$
$$\cdots\cdots$$
$$S_{2k+1} = \{(\bar{\alpha}, a) \mid \bar{\alpha} \in S, \text{ 且} a > \psi_k(\bar{\alpha})\}.$$

现在, 我们给出 "柱形代数分解" 的定义如下.

定义 9.6.3 设 n 是一个自然数. R^n 的一个柱形代数分解 是 R^n 的一个分块 $\mathcal{D}$, 它可以这样归纳地定义如下:

(1) 当 $n = 1$ 时, $\mathcal{D} = \{R\}$, 或者

$$\mathcal{D} = \{]-\infty, \alpha_1[, \{\alpha_1\},]\alpha_1, \alpha_2[, \{\alpha_2\}, \cdots,]\alpha_{r-1}, \alpha_r[, \{\alpha_r\},]\alpha_r, +\infty[\},$$

其中 $\alpha_1 < \cdots < \alpha_r$ 是 R 中 F 上代数元, 且 $]\beta, \gamma[$ 表示端点为 β 和 γ 的开区间.

(2) 如果 $\{S_1, \cdots, S_r\}$ 是 R^{n-1} 的一个柱形代数分解, 那么 $\bigcup\limits_{1 \leqslant i \leqslant r} \mathcal{D}_i$ 是 R^n 的一个柱形代数分解, 这里 $\mathcal{D}_i = \{S_i \times R\}$, 或者对于有限个 S_i 到 R 的连续半代数映射 $\psi_{i1} < \cdots < \psi_{ik_i}$, $\mathcal{D}_i$ 是柱形 $S_i \times R$ 关于 $\psi_{i1} < \cdots < \psi_{ik_i}$ 的分解, $i = 1, \cdots, r$.

对于 R^n 的一个柱形代数分解 $\mathcal{D} = \{S_1, \cdots, S_r\}$, $\mathcal{D}$ 中每个成员 $S_i (i = 1, \cdots, r)$ 称作 $\mathcal{D}$ 的一个胞腔 . 容易证明: 在柱形分解中, 每个胞腔都半代数同胚于超立方体 $]0, 1[^d$, 其中 $d \geqslant 0$, 从而每个胞腔都是半代数连通的. 此外, R^n 的一个有限子集 Δ 称作柱形代数分解 $\mathcal{D}$ 的一个样本 , 如果 $\Delta = \{\bar{\alpha}_1, \cdots, \bar{\alpha}_r\}$, 其中 $\bar{\alpha}_i \in S_i$, $i = 1, \cdots, r$. 此时, 称 $\bar{\alpha}_i$ 是 S_i 的一个样本点 , $i = 1, \cdots, r$.

定义 9.6.4 设 A 是 $F[x_1, \cdots, x_n]$ 的一个有限子集. R^n 的一个柱形代数分

解 $\mathcal{D}$ 称作是 A- 不变的，如果在 $\mathcal{D}$ 的每个胞腔上， A 是不变的.

定理 9.6.4 设 A 是 $F[x_1,\cdots,x_n]$ 的一个有限子集，则有一个有效方法，可计算出

(1) R^n 的一个 A- 不变的柱形代数分解 $\mathcal{D}_n$;

(2) $\mathcal{D}_n$ 的一个样本 Δ_n.

证明 对 n 施用归纳法. 当 $n=1$ 时， $A\subset F[x_1]$. 若 A 中所有非零多项式在 R 中无根，则 $\mathcal{D}_1=\{R\}$ 是 R 的一个柱形分解，而 $\{0\}$ 为 $\mathcal{D}_1$ 的一个样本点. 若 A 中所有非零多项式在 R 中的全部相异根为 $\alpha_1<\cdots<\alpha_r$, 则 R 有如下柱形分解:

$$\mathcal{D}_1=\{]-\infty,\alpha_1[,\{\alpha_1\},]\alpha_1,\alpha_2[,\{\alpha_2\},\cdots,]\alpha_{r-1},\alpha_r[,\{\alpha_r\},]\alpha_r,+\infty[\}.$$

显然， $\mathcal{D}_1$ 是 A- 不变的. 同时， $\mathcal{D}_1$ 的一个样本可取为

$$\Delta_1=\left\{\alpha_1-1,\alpha_1,\frac{\alpha_1+\alpha_2}{2},\alpha_2,\cdots,\frac{\alpha_{r-1}+\alpha_r}{2},\alpha_r,\alpha_r+1\right\}.$$

假定定理对于 $F[x_1,\cdots,x_{n-1}]$ 中每个有限子集都成立. 现对于 $F[x_1,\cdots,x_n]$ 的有限子集 A, 首先可计算 A 的投影 $\mathrm{Proj}(A;x_n)$. 由归纳假定，可有效地计算 R^{n-1} 的一个 $\mathrm{Proj}(A,x_n)$- 不变的柱形代数分解 $\mathcal{D}_{n-1}$ 和它的一个样本 Δ_{n-1}. 根据定理 9.6.3, 对于每个 $S\in\mathcal{D}_{n-1}$, A 的根在 S 上是可描绘的，且存在 S 到 R 的连续半代数映射 $\psi_1<\cdots<\psi_k$, 使得定理 9.6.3 中的要求被满足. 令 $\mathcal{D}_S$ 是柱形 $S\times R$ 关于 $\psi_1<\cdots<\psi_k$ 的分解. 若 $\Delta_{n-1}\cap S=\{\bar{\alpha}_S\}$, 则构造 R^n 的如下子集:

$$\begin{aligned}\Delta_S= & \left\{(\bar{\alpha}_S,\alpha_1-1),(\bar{\alpha}_S,\alpha_1),\left(\bar{\alpha}_S,\frac{\alpha_1+\alpha_2}{2}\right),\right.\\ & \left.(\bar{\alpha}_S,\alpha_2),\cdots,\left(\bar{\alpha}_S,\frac{\alpha_{r-1}+\alpha_r}{2}\right),(\bar{\alpha}_S,\alpha_r),(\bar{\alpha}_S,\alpha_r+1)\right\}.\end{aligned}$$

这里 $\alpha_1<\cdots<\alpha_r$ 为 $\{f(\bar{\alpha}_S,x)\mid f\in A\}$ 中所有非零多项式在 R 中的全部相异根.

此时易证， $\bigcup\limits_{S\in\mathcal{D}_{n-1}}\mathcal{D}_S$ 是 R^n 的一个 A- 不变的柱形代数分解，且 $\bigcup\limits_{S\in\mathcal{D}_{n-1}}\Delta_S$ 是它的一个样本. 由归纳原理，定理获证.

应该指出，在上面定理证明中，我们还使用这样一个前提条件： R_0 上单元多项式的实根 (即在 R_0 中的根) 都可有效地求出，这里 R_0 是 F 在 R 中的代数闭包. 实际上，当 $(F,\leqslant)$ 是一个可计算序域时， R_0 上单元多项式的实根都具有某种有效表示. 因而，上面定理特别适用于 F 为有理数域这一情形.

柱形代数分解具有许多方面的应用，尽管它不可避免地会涉及到繁杂计算. 下面的简单例子表明，柱形代数分解可用来判定序域语言中一个语句是否适合实闭

域.

例 证明：对于任意实闭域 R,

$$(R,<)\models(\forall b)(\forall c)\Big(b^2-4c\geqslant 0\longleftrightarrow\exists x(x^2+bx+c=0)\Big),$$

这里 $<$ 是 R 的惟一序.

证明 由转移定理 (定理 7.3.7) 知，只须证明如下事实：

$$(R_0,<)\models(\forall b)(\forall c)\Big(b^2-4c\geqslant 0\longleftrightarrow\exists x(x^2+bx+c=0)\Big),$$

这里， R_0 是有理数域 $\mathbb{Q}$ 关于其惟一序的实闭包.

令 $A=\{b^2-4c,x^2+bx+c\}$, 则 A 是多项式环 $\mathbb{Q}[x,b,c]$ 的一个有限子集. 根据多项式集的投影的定义，可计算出

$$\begin{aligned}A_1&=\mathrm{Proj}(A;x)=\{b^2-4c,b,c,2,c^2\},\\A_2&=\mathrm{Proj}(A_1;b)=\{1,2,c,c^2,-4c\},\end{aligned}$$

显然， A_2 中所有多项式在 R 中只有惟一根 $c=0$. 从而， R_0 的一个 A_2- 不变的柱形代数分解的样本为 $\{-1,0,1\}$. 当 $c=-1,\ 0,\ 1$ 时， A_1 中多项式在 R_0 中的根集分别为 $\{0\},\{0\},\{0,4\}$. 从而 R_0^2 的一个 A_1- 不变的柱形代数分解 $\mathcal{D}$ 的样本为

$$\begin{aligned}\varDelta=\ \ &\{(-1,-1),(-1,0),(-1,1),(0,-1),\\&(0,0),(0,1),(1,-1),(1,0),(1,2),(1,4),(1,5)\}.\end{aligned}$$

当 (c,b) 依次取 $\varDelta$ 中的点时，计算 b^2-4c 的值，同时用 Sturm 定理 (或其他方法) 判定 x^2+bx+c 在 R_0 中是否有根. 从而获得下表.

(c,b)	b^2-4c	x^2+bx+c
$(-1,-1)$	>0	在 R_0 中有根
$(-1,0)$	>0	在 R_0 中有根
$(-1,1)$	>0	在 R_0 中有根
$(0,-1)$	>0	在 R_0 中有根
$(0,0)$	$=0$	在 R_0 中有根
$(0,1)$	>0	在 R_0 中有根
$(1,-1)$	<0	在 R_0 中无根
$(1,0)$	<0	在 R_0 中无根
$(1,2)$	$=0$	在 R_0 中有根
$(1,4)$	>0	在 R_0 中有根
$(1,5)$	>0	在 R_0 中有根

由上表可见，当 $b^2-4c\geqslant 0$ 时， x^2+bx+c 在 R_0 中有根；否则， x^2+bx+c 在 R_0 中无根. 由于在 $\mathcal{D}$ 的每个胞腔上， x^2+bx+c 在 R_0 中的根是可描绘的.

因而，多项式 x^2+bx+c 在 $\mathcal{D}$ 的某个胞腔上是否有在 R_0 中的根，完全取决于当 (c,b) 取该胞腔的样本点时，x^2+bx+c 是否在 R_0 中有根．注意到，b^2-4c 在 $\mathcal{D}$ 的每个胞腔上保持不变．于是，上面欲证的事实成立．因而，例题的结论获证．

参考文献

[1] E Artin. Über die Zerlegung definiter Funktionen in Quadrate. Abh. Math. Sem. Univ. Hamburg, 1927,5: 100~115

[2] E Artin and O Schreier. Algebraische Konstruktion reeller Körper. Abh. Math. Sem. Univ. Hamburg, 1927,5: 85~99

[3] E Artin and O Schreier. Eine Kennzelchnung der reell algeschlossennen Körper. Abh. Math. Sem. Univ. Hamburg, 1927,5: 225~231

[4] R Baer. Über nicht-archimedisch geordnete Körper. Sitz. Ber. der Heidelberger Akad. 1927,8, Abh: 3~13

[5] R Baer. Dichte, Archimedizität und Starrheit geordneter Körper. Math Ann, 1970,188: 165~205

[6] S A Basarab. On a class of preordering of higher level. Manuscripta Math, 1982,37:2: 163~210

[7] E Becker. Euklidische Körper und euklidische Hullen von Körpern. J. reine angew. Matrh, 1974,268/269: 41~52

[8] E Becker. Hereditarily pythagorean fields, infinite Harrison primes and sums of 2^n-th powers. Bull Amer Math Soc, 1978,84: 278~280

[9] E Becker. *Hereditarily Pythagorean Fields and Orderings of Higher Level. IMPA Lecture Notes. No. 29*, Rio de Janeiro, 1978

[10] E Becker. Formal-reeller Körper mit streng-auflösbarer absiluter Glaisgruppe, Math Ann, 1978,238: 203~206

[11] E Becker. Partial orders on a field and valuation rings. Comm. in Algebra, 1979,7: 1937~1976

[12] E Becker. Summen n-ter Potenzen in Körpern. J reine angew Math, 1979,307/308: 8~30

[13] E Becker. Valuations and real places in the theory of formally real fields. *Lecture Notes in Math. 959*, Berlin-Heidelberg-New York, Springer-Verlag, 1982: 1~40

[14] E Becker. The real holomorphy ring and sums of $2n$-th powers. *Lecture Notes in Math. 959*, Berlin-Heidelberg-New York, Springer-Verlag, 1982: 139~181

[15] E Becker. Extended Artin-Schreier theory of fields. Rocky Mountain J Math, 1984,14: 881~897

[16] E Becker and K-J Spitzlay. Zum Satz von Artin-Schreier über die eindeutigkeit des reellen Abschlusses eines geordneten Körpers. Comm Math Helv, 1975, 50: 81~87

[17] E Becker and E Köpping. Reduzierte quadratische Formen und Semiordnungen reeller Körper. Abh Math Sem Univ Hamburg, 1977,46: 17~143

[18] E Becker and L Bröcker. On the description of the reduced Witt ring. J Algebra, 1978,52: 328~346

[19] E Becker, J Harman and A Rosenberg. Signatures of fields and extension theory. J reine angew Math, 1982,330: 53~75

[20] E Becker and N Schwartz. Zum Darstellungssatz von Kadison-Dubois. Arch Math, 1983,40: 421~428

[21] E Becker, V Powers and T Wörmann, Deciding positivity of real polynomials. In: Real Algebraic Geometry and Ordered Fields. *Contemporary Math 253*, Providence R I, Amer Math Soc, 2000: 19~23

[22] T Becker, V Weispfenning and H Kredel. *Gröbner Bases: A computational approach to commutative algebra.* New York-Berlin -Heidelberg. Springer-Verlag, 1993

[23] J Bochnak. Sur le 17éme probléme de Hilbert pour les fonctions de Nash. Proc Amer Math Soc, 1978,71: 183~188

[24] J Bochnak and G Efroymson. Real algebraic geometry and the 17-th Hilbert problem. Math. Ann, 1980,251: 213~241

[25] J Bochnack J, M Coste and M F Roy. *Real Algebraic Geometry*. New York-Berlin-Heidelberg, Springer-Verlag, 1998

[26] L Bröcker. Über eine Klasse pythagoreischer Körper. Arch Math, 1972,23: 405~407

[27] L Bröcker. Zur Theorie der quadratische Formen über formal reellen Körpern. Math Ann, 1974,210: 233~256

[28] L Bröcker. Characterization of fans and hereditarily pythagorean fields. Math Zeit, 1976,151: 149~163

[29] L Bröcker. Über die Anzahl der Anordnungen eines kommutativen Körpers. Arch Math, 1977,29: 458~464

[30] L Bröcker. Über die Pythagoraszahl eines Körpers. Arch Math, 1978,34: 133~136

[31] R Brown. Real places and ordered fields. Rocky Mountain J Math, 1971,1: 633~636

[32] R Brown. Superpythagorean fields. J Algebra, 1976,42: 483~494

[33] R Brown. The reduced Witt ring of a formally real field. Trans Amer Math Soc, 1977,230: 257~292

[34] R Brown. Real closures of fields at orderings of higher level. Pacific J Math, 1987,127:2: 261~278

[35] R Brown. The behavior of chains of orderings under field extensions and places. Pacific J Math, 1987,127:2: 281~297

[36] R Brown. T C Craven and M J Pelling. Ordered fields satisfying Rolle's theorem. Illinois J Math, 1986,30:1: 66~78

[37] G Brumfiel. *Partially Ordered Rings and Semi-algebraic Geometry. Lecture Note Series of London Math Soc.* Cambridge Univ Press, 1979

[38] B F Caviness and J R Johnson(eds.). *Quantifier Elimination and Cylindrical Algebraic Decomposition.* Wien-New York: Springer-Verlag, 1998

[39] G E Collins. Quantifier elimination for the elementary theory of real closed fields by cylindrical algebraic decomposition. Lecture Notes Comput. Sci, 1975,33: 85~121

[40] P Conrad. On ordered division rings. Proc Amer Math Soc, 1954,5: 323~328

[41] P Conrad and J Dauns. An imbedding theorem for lattice-ordered fields. Pacific J Math, 1969,30: 385~398

[42] M Coste and M F Roy. Thom's lemma, the coding of real algebraic numbers and the compution of the topology of semi-algebraic sets. J Symbol Comput, 1988,5:1: 121~129

[43] T C Craven. The topological space of orderings of a rational function field. Duke Math J, 1974,41: 339~347

[44] T C Craven. The Boolean space of orderings of a field. Trans Amer Math Soc, 1975,209: 225~235

[45] T C Craven. Existence of SAP extension fields. Arch Math, 1977,29: 594~597

[46] T C Craven. Intersections of real closed fields. Canad J Math, 1980,32:2: 431~440

[47] T C Craven and G Csordas. Location of zeros, Part I: real polynomials and entire functions. Illinois J Math, 1983,27:2: 244~278

[48] T C Craven and G Csordas. Location of zeros, Part II: ordered fields. Illinois J Math, 1983,27:2: 279~299

[49] Dai Zhizhong and Zeng Guangxing. Valuation theory and generalizations of Hilbert's 17th problem. Lecture Notes Pure Appl Math, 1996,181: 39~50

[50] 戴执中. 赋值论概要. 北京：人民教育出版社， 1981

[51] 戴执中. 关于有序域的几点注记. 数学研究与评论. 1982,2:2: 7~10

[52] 戴执中. 域论. 北京：高等教育出版社， 1990

[53] 戴执中，曾广兴. Hilbert 第十七问题. 南昌：江西教育出版社， 1990

[54] J A de Loera and F Santos. An effective version of Pólya's theorem on positive definite forms. J Pure Appl Algebra, 1996,108: 231~140

[55] J A de Loera and F Santos. Erratum to: "An effective version of Pólya's theorem on positive definite forms". J Pure Appl Algebra, 2001,155: 309~310

[56] C N Delzell. A continuous, constructive solution to Hilbert's 17th problem. Invent Math, 365~384

[57] C N Delzell. Continuous, piecewise-polynomial functions which solve Hilbert's 17th problem. J reine angew Math, 1993,440: 157~173

[58] J Dieudonné. Sur les corps ordonnables. Bol Soc Mat Sáo Paulo, 1946,1: 69~75

[59] J Dieudonné. Complément á mon article "Sur les corps ordonnables". Bol Soc Mat Sáo Paulo, 1947,2: 35

[60] J Diller and A Dress. Zur Galoistheorie pythagoreischer Körper. Arch Math, 1965,16: 148~152

[61] D Z Djokovic. Positive semidefinite matrices as sums of squares. Linear Algebra and Its Appl, 1976,14: 37~40

[62] D Z Djokovic. Artin-Schreier theory for positive semidefinite symmetric and hermitian matrices. Glasnik Mat Ser III, 1977,12: 9~20

[63] A Dress. On orderings and valuations of fields. Geometriae Dedicata, 1977,6: 259∼266

[64] D W Dubois. Note on Artin's solution of Hilbert's 17-th problem. Bull Amer Math Soc, 1967,73: 540∼541

[65] D W Dubois. A note on David Harrison's theory of preprimes. Pacific J Math, 1967,21: 15∼19

[66] D W Dubois. Second note on David Harrison's theory of preprimes. Pacific J Math, 1968,24: 57∼68

[67] D W Dubois. A Nullstellensatz for ordered fields. Arkiv Math, 1969,8: 111∼114

[68] D W Dubois. Infinite primes and ordered fields. Dissertations Math, 1970,69: 5∼40

[69] D W Dubois. Second note on Artin's solution of Hilbert's 17th problem, order spaces. Pacific J Math, 1981,97:2: 857∼871

[70] D W Dubois and T Récio. Order extensions and real algebraic geometry. *Contemporary Math 8*, 1982: 265∼288

[71] R Elman and T Y Lam. Quadratic forms over formally real fields and pythagorean fields. Amer J Math, 1972,94: 1155∼1194

[72] R Elman and T Y Lam. Quadratic forms under algebraic extensions. Math Ann, 1976,219: 21∼42

[73] R Elman, T Y Lam and A Prestel. On some Hasse principles over formally real fields. Math Zeit, 1973,134: 291∼301

[74] R Elman, T Y Lam and A Wadsworth. Orderings under field extensions. J reine angew Math, 1979,306: 7∼27

[75] R Elman, T Y Lam and A Wadsworth. Function fields of Pfister forms. Invent Math, 1979,51: 61∼75

[76] O Endler. *Valuation Theory*. New York: Springer-Verlag, 1972

[77] A J Engler. Formally real fields with a simple description of the absolute Galois group. Manuscripta Math, 1986,56:1: 71∼87

[78] J M Gamboa. Some new results on ordered fields. J Algebra, 1987,110: 1∼12

[79] J M Gamboa and T Recio. Ordered fields with the dense orbits property. J Pure Appl Algebra, 1983,30: 237∼246

[80] W D Geyer. Unendliche algebraische Zahlköper, über denen jede gleichung auflösbar von beschränkter Stufe ist. J Number Theory, 1969,1: 346∼374

[81] R Gilmer. Extension of an order to a simple transcendental extension. *Contemporary Math 8*, 1982: 113∼118

[82] D Gondard and P Ribenboim. Sur le 17éme probléme de Hilbert. C R Acad Sci Paris, 1973,227: 303∼304

[83] D Gondard and P Ribenboim. Fonctions définites positives sur les variétés réelles. Bull Sci Math 2e série, 1974,98: 39∼47

[84] D Gondard and P Ribenboim. Le 17éme probléme de Hilbert pour les matrices. Bull Sci Math 2e série, 1974,98: 49∼56

[85] M Griffin. The pythagorean closures of fields. Math Scand, 1976,38: 177~191

[86] H Gross and P Hafner. Über die eindeutigkeit des reellen Abslchlusses eines angeordneten Körperns. Comment Math Helv, 1969,44: 491~494

[87] W Habicht. Über die Zerlegung strikte definiter Formen in Quadrate. Comm Math Helv, 1940,12: 317~322

[88] J Harman. Chains of higher level orderings. *Contemporary Math. 8*, 1982: 141~174

[89] D Harrison. *Finite and Infinite primes for Rings and Fields. Mem Amer Math Soc, No. 68*, 1968

[90] D Harrison and H Warner. Infinite primes of fields and completions. Pacific J Math, 1973,45: 201~206

[91] H E Heatherly. Ordered fields of arbitrary cardinality. Math Student, 1974/1975,42: 223~224

[92] A Heck. *Introduction to Maple*. New York-Berlin-Heidelberg. Springer-Verlag, 1993

[93] D Hilbert. Über die Darstellung definiter Formen als Summe von Formenquadraten. Math Ann, 1888,32: 342~350

[94] D Hilbert. Über ternäte definite Formen. Acta Math, 1893,17: 169~197

[95] D Hilbert. Mathematische Probleme. Arch Math Physik I, 1901: 44~63, 213~277

[96] Jr S Holland. Orderings and square roots of *-fields. J Algebra, 1977,46: 207~219

[97] T Iwakami and D Kijima. Spaces of orderings and quadratic extensions of fields. Hiroshima Math J, 1986,16:1: 21~31

[98] B Jacob. A Nullstellensatz for $\mathbb{R}((t))$. Comm in Algebra, 1980,8: 1083~1094

[99] B Jacob. On the structure of pythagorean fields. J Algebra, 1981,68: 247~267

[100] B Jacob. The model theory of generalized real closed fields. J reine angew Math, 1981,323: 213~220

[101] B Jacob. Fans, real valuations and heraditarily pythagorean fields. Pacific J Math, 1981,93: 95~105

[102] J R Joly. Sommes des puissances d-iémes dans un anneau commutatif. Acta Arith, 1970,17: 37~114

[103] I Kaplansky. *Infinite Abelian Groups*. Ann Arbor. Univ of Michigan Press, 1969

[104] J L Kelley. *General Topology*. New York-Heidelberg-Berlin. Springer-Verlag, 1955

[105] D Kijima. Cuts of ordered fields. Hiroshima Math J, 1987,17:2: 337~347

[106] D Kijima and M Nishi. Maximal ordered fields of rank n. Hiroshima Math J, 1987,17:1: 157~167

[107] D Kijima, M Nishi and M Sakaibara. Maximal ordered fields of rank n, II. Hiroshima Math J, 1987,18:1: 219~225

[108] M Knebusch. On the uniqueness of real closures and the existence of real places. Comment. Math Helv. 1972,47: 260~269

[109] M Knebusch. On the extension of real places. Comment Math Helv, 1973,48:3: 354~369

[110] M Knebusch. Generalization of a theorem of Artin-Pfister to arbitrary semilocal rings and related topics. J Algebra, 1975,36: 46~67

[111] M Knebusch. Real closures of commutative rings I. J reine angew. Math, 1975,274/275: 61~89

[112] M Knebusch. Real closures of commutative rings II. J reine angew. Math, 1976,286/287: 280~321

[113] M Knebusch and M Wright. Bewertungen mit reeller Henselisierung. J reine angew. Math, 1976,286/287: 314~321

[114] M Knebusch and C Scheiderer. *Einführung in die reelle Algebra*. Braunschweig. Friedr. Vieweg & Sohn, 1989

[115] J Krivine. Anneaux préordonnés. J d'Analyse Math, 1964,12: 307~326

[116] W Krull. Allgemeine Bewertungstheorie. J reine angew. Math, 1932,167: 160~196

[117] M Krüskemper. On real local-global principles. Math. Zeit, 1990,204: 145~151

[118] T Y Lam. *The Algebraic Theory of Quadratic Forms*. W A Benjamin. Reading. Massachusetts, 1973

[119] T Y Lam. *The Theory of Ordered Fields. Lecture Notes in Pure and Appl Math* 55. New York. M Dekker, 1980: 1~152

[120] T Y Lam. *Orderings. Valuations and Quadratic Forms. CBMS Regional Conf. Series in Math* 52. Amer Math Soc. Providence. R I, 1983

[121] T Y Lam. An introduction to real algebra. Rocky Mountain J Math, 1984,14: 767~814

[122] S Lang. On quasi algebraic closure. Ann Math, 1952,55: 373~390

[123] S Lang. The theory of real places. Ann Math, 1953,57: 378~391

[124] D Laugwitz. Eine nicht-archimedische erweiterung angeordneter Körper. Math Nachr, 1968,37: 225~236

[125] D Laugwitz. Bemerkungen über Stetigkeit und angeordnete Körper. Demonstratio Math, 1973,6: 191~209

[126] A Lax and P D Lax. On sums of squares. Linear Alg and its Appl. 1978,20: 71~75

[127] J Leicht and F Lorenz. Die Primideale des Wittschen Ringes. Invent Math, 1970,10: 378~391

[128] 梁松新，曾广兴. 无限维空间中的实零点定理. 数学学报， 1996,39:3: 336~344

[129] F Lorenz. *Quadratische Formen über Körpern. Lecture Notes in Math. 130*, Springer-Verlag, 1970

[130] F Lorenz. Quadratische Formen und die Artin-Schreiersche Theorie der formal reellen Körper. Bull Soc Math France Mem, 1976,48: 61~73

[131] K McKenna. New facts about Hilbert's 17th problem. Lecture Notes in Math 498, Berlin-New York, Springer-Verlag, 1975: 220~230

[132] M Marshall. Some local-global principles for formally real fields. Canad. J Math, 1977,29: 606~614

[133] M Marshall. Classification of finite spaces of orderings. Canad. J Math, 1979,31:

320~330

[134] M Marshall. Quotients and inverse limits of spaces of orderings. Canad. J Math, 1979,31: 604~616

[135] M Marshall. The Witt ring of a space of orderings. Trans Amer Math Soc, 1980,258: 505~521

[136] M Marshall. Spaces of orderings. IV, Canad. J Math, 1980,32: 603~627

[137] B Mishra. *Algorithm Algebra. Texts and Monographs in Computer Sci*, New York-Berlin-Heidelberg. Springer-Verlag, 1993

[138] M Nagata. Some remarks on ordered fields. Japan J Math, 1975,1: 1~4

[139] M Nagata. *Field Theory*. New York. Marcel Dekker, Inc, 1977

[140] R Neuhaus. Compution of real radicals of polynomial ideals. J Pure Appl. Algabra, 1998,124: 261~280

[141] B H Neumman. On ordered division rings. Trans Amer Math Soc, 1949,66: 202~252

[142] M J Pelling. Solutions of advanced problems. No. 5861, Amer Math Monthly, 1981,88: 150~152

[143] A Pfister. Multiplicative quadratische Formen. Arch Math, 1965,16: 363~370

[144] A Pfister. Quadratische Formen in beliebigen Körpern. Invent Math, 1966,1: 116~132

[145] A Pfister. Zur Darstellung definiter Funktionen als Summe von Quadraten. Invent Math, 1967,4: 229~237

[146] A Pfister. Hilbert's seventeenth problem and related problems on definite forms. in *Mathematical Developments Arising from Hilbert Problems*. (ed F Browder), Proc Symp Pure Math, 28, 483~489, Amer Math Soc, Providence, R I, 1976

[147] A Pfister. *Quadratic Forms with Applications to Algebraic Geometry and Topology. London Math Soc Lecture Note Series* 217, Cambridge Univ Press, 1995

[148] G Pólya. Über positive Darstellung von Polynomen. Vierteljahrsschrift Natur. Ges in Zürich, 1928,73: 141~145

[149] V Powers. Hilbert's 17th problem and the champagne problem. Amer Math Monthly, 1996,103:10: 879~887

[150] A Prestel. Quadratische Semi-Ordnungen und quadratische Formen. Math Zeit, 1973,133: 319~342

[151] A Prestel. A local-global principle for quadratic forms. Math Zeit, 1975,142: 91~95

[152] A Prestel. Local-global principles for quadratic forms over function fields. in Proc. Quad Form Conf(ed G Orzech), Queen's Papers in Pure and Applied Math, 1976,46: 595~612

[153] A Prestel. Sums of squares over fields. Soc Brasil Rio de Janeiro, 1979, 33~44

[154] A Prestel. Decidable theories of preordered fields. Math Zeit, 1982,258: 481~492

[155] A Prestel. *Lectures on Formally Real Fields. Lecture Notes in Math, 1093*, Berlin-Heidelberg-New York: Springer-Verlag, 1984

[156] A Prestel and C N Delzell. *Positive Polynomials: From Hilbert's 17th Problem to Real*

Algebra. Berlin-Heidelberg-New York. Springer-Verlag, 2001

[157] A Prestel and M Ziegler. Erblich eukidische Körper. J reine angew. Math, 1975,274/275: 196～205

[158] S Priess-Crampe. Zum Hahnschen Einbettungssatz für angeordnete Körper. Arch Math, 1973,24: 607～614

[159] C Procesi. Positive symmetric functions. Adv in Math, 1978,29: 219～225

[160] C Procesi and M Schacher. A non-commutative real Nullstellensatz and Hilbert's 17th problem. Ann Math, 1976,104: 395～406

[161] P Ribenboim. On orderable fields. Math Nachr, 1969,40: 343～355

[162] P Ribenboim. Le théoreme des zéros pour les corps ordonnés. Sem Dubrell-pisot, 24[e] année, Exp. 17 , 1970/1971

[163] P Ribenboim. 17éme probléme de Hilbert. Bol Soc Bras Mat, 1974,5: 63～67

[164] P Ribenboim. Quelques developpments récents du 17[e] probléme de Hilbert. Soc Math de France Asterique, 1975,24/25: 237～241

[165] J J Risler. Une caracterization des idéaux des variétés algebriques réeles. C R Acad Sci Paris, 1970,271: 1171～1173

[166] B Reznick. Uniform denominators in Hilbert's 17th problem. Math Zeit, 1995,220: 75～97

[167] B Reznick. Some concrete aspects of Hilbert's 17th problem. *Séminarie de Structures Algébriques Ordonnées. Vol. 56*, Équipe de Logique Mathématique, Université Paris VII, 1996

[168] A Robinson. On ordered fields and definite functions. Math Ann, 1955,130: 257～271

[169] A Robinson. Further remarks on ordered fields and definite functions. Math Ann, 1956,130: 405～409

[170] W Roger. Extending orderings on formally real fields. Arch Math, 1975,26:6: 611～614

[171] J M Ruiz. On Hilbert's 17th problem and real Nullstellensatz for global analytic functions. Math Zeit, 1985,190: 447～454

[172] J M Ruiz. A remark of fields with the dense orbits property. Pacific J Math, 1986,121:1: 189～192

[173] C Scheiderer. Real algebra and its applications to geometry in the last 10 years. *Lecture Notes in Math.* 1524, Springer-Verlag, Berlin-Heidelberg-New York, 1992: 75～96

[174] J Schmid. Eine Bemerkung zu den höheren Pythageraszahlen reeller Körper. Manuscripta Math, 1988,61:2: 195～202

[175] H W Schülting. Real points and real places. *Contemporary Math 8*, 1982: 289～294

[176] N Schwartz. The strong topology on real algebraic varieties. *Contemporary Math 8*, 1982: 297～325

[177] N Schwartz. Chain signatures and real closures. J reine angew. Math, 1984,347: 1～20

[178] D Scott. On completing ordered fields, in *Applications of Model Theory to Algebra, Analysis and Probability* (ed. W. Luxemburg). Hoit-Rinehart, New york, 1969:

274~278

[179] P Scowcroft. Some continuous Positivstellensätze. J Algebra, 1989,124: 521~532

[180] A Seidenberg. A new decision method for elementary algebra. Ann Math, 1954,60:2: 365~374

[181] H Shafarevich. *Basic Algebraic Geometry 1: Varieties in Projective Space*, 2nd ed, New York-Berlin-Heidelberg, Springer-Verlag, 1994

[182] O Simon, Aspects quantitatifs de Nullstellensätze et de Positvstellensätze, Nombers de Pythagore. Comm in Algebra, 1989,17:3: 637~667

[183] G Stengle. A Nullstellensatz and a Positivstellensatz in semialgebraic geometry. Math Ann, 1974,207: 87~97

[184] G Stengle. Integral solution of Hilbert's seventeenth problem. Math Ann, 1979,246: 33~39

[185] T Szele. On ordered skew fields. Proc Amer Math Soc, 1952,3: 410~413

[186] A Tarski. *A Decision Method for Elementary Algebra and Geometry*. Berkeley, Rand Corporation, 1951

[187] O Taussky. Sums of squares. Amer Math Monthly, 1970,77: 805~830

[188] C C Tsen. Zur Stufentheorie der quasialgebraisch Abgeschlossenheit kommutativer Körper. J Chinese Math Soc, 1936,1: 81~92

[189] T M Viswanathan. Ordered fields and sign-changing polynomials. J reine angew. Math, 1977,296: 1~9

[190] R von Chossy and S Priess-Crampe. Ordnungswerträgliche Bewertunggen eines angeordneten Körpers. Arch Math, 1975,26: 372~387

[191] R Ware. Extending orderings on formally real fields. Arch Math, 1975,26: 611~614

[192] R Ware. Hasse principles and the u-invariant over formally real fields. Nagoya Math J, 1976,61: 117~125

[193] E Witt. Zerlegung reeller algebraischer Funktionen in Quadrate, Schiefkörper über reellem Funktionenkörper. J reine angew. Math, 1933,171: 4~11

[194] E Witt. Theorie der quadratischen Formen in beliebigen Körpern. J reine angew. Math, 1937,176: 31~44

[195] Wu Wen-tsun. Mechanical theorem proving in geometries: Basic principle. Wien-New York, Springer-Verlag, 1994

[196] Wu Wen-tsun. *Mathematics Mechanization: Mechanical Geometry Theorem-Proving, Mechanical Geometry Problem-Solving and Polynomial Equations-Solving*. Science Press/Kluwer Academic Publishers, 2000

[197] 吴文俊. 几何定理机器证明的基本原理. 北京：科学出版社， 1984: 208~228

[198] Yang Lu, Hou Xiaorong and Zeng Zhenbing. A complete discrimination system for polynomials. Science in China, Series E, 1996, 36 ： 6: 628~646

[199] 杨路，张景中，候晓荣. 非线性代数方程组与定理机器证明. 上海：上海科技教育出版社，1996

[200] O Zariski and P Samuel. *Commutative Algebra. Vol 1*, New York-Berlin-Heidelberg, Springer-Verlag, 1958

[201] Zeng Guangxing. A new proof of McKenna's theorem. Proc Amer Math Soc, 1988,102: 827~830

[202] Zeng Guangxing. A characterization of preordered fields with the weak Hilbert property. Proc Amer Math Soc, 1988,104: 335~342

[203] Zeng Guangxing. On preordered fields related to Hilbert's 17th problem. Math Zeit, 1991,206: 145~151

[204] Zeng Guangxing. Homogeneous Stellensätzen in semialgebraic geometry. Pacific J Math, 1989,136:1: 103~122

[205] Zeng Guangxing. A problem about the weak Hilbert property. Acta Math Sinica (New Series), 1998,14:4: 481~486

[206] Zeng Guangxing. Computation of generalized real radicals of polynomial ideals. Scienc in China, Series A, 1999,42:3: 272~280

[207] Zeng Guangxing. Nonstandard decision methods for the solvability of real polynomial equations. Science in China, Series A, 1999,42:12: 1251~1261

[208] Zeng Guangxing. Valuations and convex subrings in a commutative ring with higher level preordering. Math Zeit, 2001,237: 219~234

[209] Zeng Guangxing. A rigorous proof of Craven's theorem. to appear

[210] Zeng Guangxing. A nonstandard decision method for algebraic equations having real solutions. to appear

[211] Zeng Guangxing. An effective decision method for semidefinite polynomials. to appear

[212] 曾广兴. 带核实域上的正定函数. 数学进展, 1988,17:3: 285~289

[213] 曾广兴. 带核实赋值环上的正定多项式. 数学学报, 1988,31:5: 634~644

[214] 曾广兴. Lang 同态定理的一个推广. 科学通报, 1988,8: 570~572

[215] 曾广兴. 具有弱 Hilbert 性质的域之赋值刻划. 数学学报, 1989,32:5: 690~701

[216] 曾广兴. 适合无限维实零点定理的序域之刻划 I. 数学学报, 1999,42:1: 125~132

[217] 曾广兴. 适合无限维实零点定理的序域之刻划 II. 数学学报, 1999,42:2: 281~288

索 引

(中文部分按汉语拼音字母顺序为序，外文部分按字母顺序为序，各词条附英文)

H

J

K

L

M

O

Q

R

S

T

W

X

Y

Z